CMS Books in Mathematics

Richard Kane

Reflection Groups and Invariant Theory

Canadian Mathematical Society
Société mathématique du Canada

Canadian Mathematical Society
Société mathématique du Canada

Editors-in-Chief
Rédacteurs-en-chef
Jonathan Borwein
Peter Borwein

Springer Science+Business Media, LLC

CMS Books in Mathematics
Ouvrages de mathématiques de la SMC

1 HERMAN/KUČERA/ŠIMŠA Equations and Inequalities
2 ARNOLD Abelian Groups and Representations of Finite Partially Ordered Sets
3 BORWEIN/LEWIS Convex Analysis and Nonlinear Optimization
4 LEVIN/LUBINSKY Orthogonal Polynomials for Exponential Weights
5 KANE Reflection Groups and Invariant Theory
6 PHILLIPS Two Millennia of Mathematics
7 DEUTSCH Best Approximations in Inner Product Spaces
8 FABIAN ET AL. Functional Analysis and Infinite-Dimensional Geometry

Richard Kane

Reflection Groups and Invariant Theory

Springer

Richard Kane
Department of Mathematics
University of Western Ontario
London, Ontario N6A 5B7
Canada
rkane@julian.uwo.ca

Mathematics Subject Classification (2000): 13A50, 51F15

Library of Congress Cataloging-in-Publication Data
Kane, Richard M., 1944–
Reflection groups and invariant theory / Richard Kane.
p. cm. — (CMS books in mathematics ; 5)
Includes bibliographical references and index.
ISBN 978-1-4419-3194-8 ISBN 978-1-4757-3542-0 (eBook)
DOI 10.1007/978-1-4757-3542-0
1. Reflection groups. 2. Invariants. I. Title. II. Series.
QA177 .K36 2001
512′2—dc21 2001020046

Printed on acid-free paper.

Production managed by Allan Abrams; manufacturing supervised by Jacqui Ashri.
Photocomposed copy prepared using the author's LaTeX2e files.

9 8 7 6 5 4 3 2 1

ISBN 978-1-4419-3194-8 SPIN 10751051

Contents

Introduction: Reflection groups and invariant theory

The concept of a reflection group is easy to explain. A *reflection* in Euclidean space is a linear transformation of the space that fixes a hyperplane while sending its orthogonal vectors to their negatives. A *reflection group* is, then, any group of transformations generated by such reflections. The purpose of this book is to study such groups and their associated invariant theory, outlining the deep and elegant theory that they possess.

The book can be divided into three parts. Reflection groups and their invariant theory provide the main themes of this book, and the first two parts are focused on these topics. The first thirteen chapters deal with reflection groups (Coxeter groups and Weyl groups) in Euclidean space, whereas the next thirteen chapters study the invariant theory of pseudo-reflection groups. These latter groups are generalizations of Euclidean reflection groups to the case of arbitrary vector spaces, and provide a more natural context in which to do invariant theory. The third part of the book, consisting of the last eight chapters, is a study of conjugacy classes in reflection and pseudo-reflection groups.

(I) Chapters 1–13: Reflection groups and root systems

The study of reflection groups was initiated by the work of Coxeter in the 1930s and has continued to the present. Notably, all Euclidean reflection groups possess a *Coxeter group* structure. The first eight chapters of the book detail the main results obtained for reflection groups and their associated Coxeter group structures. This includes a very explicit classification result. The principal tool employed in the analysis is that of a *root system*. A root system can be regarded as a linear algebra reformulation of the geometry of the reflecting hyperplanes. Root systems provide algebraic and combinatorial data that can be readily used to analyze reflection groups. A classification of finite Coxeter groups and reflection groups follows from this analysis.

The study of *Weyl groups* is a subtheme of the study of Euclidean reflection groups. These are the reflection groups that possess *crystallographic* root systems. The classification of Weyl groups and of crystallographic root systems is a refinement of the classification of Euclidean reflection groups. Weyl groups and crystal-

lographic root systems are discussed and classified in Chapters 9–13. These classifications are fundamental and play an important role in various areas of mathematics not treated in this book, notably in Lie theory.

(II) Chapters 14–26: Pseudo-reflection groups and invariant theory

Invariant theory has been an area of investigation for more than one hundred years. The invariant theory of reflection groups has been a significant topic since the 1950s. It arose out of the study of the homology of Lie groups. Motivated by that study, Chevalley showed that the ring of invariants of a reflection group has a very simple structure, namely that the invariants form a *polynomial algebra*. At the same time, it was realized by Shephard-Todd that this fact holds, more generally, for complex *pseudo-reflection* groups. As mentioned, pseudo-reflection groups provide the natural context in which to discuss the invariant theory of reflection groups. A comprehensive study of the invariant theory of pseudo-reflection groups was thereafter undertaken (by, among others, Bourbaki, Solomon, Springer and Steinberg) showing how invariant theory gives a great deal of information about pseudo-reflection groups, and can even be used to characterize them in many cases. In particular, the fact that the polynomial property actually characterizes pseudo-reflection groups, and that this relation holds over most fields, was presented in the Bourbaki treatment of reflection groups.

Chapters 14–26 provide a detailed treatment of pseudo-reflection groups and their invariant theory. The basic theme of the discussion is that pseudo-reflection groups have a particularly nice invariant theory and, moreover, the structure of pseudo-reflection groups is mirrored in their invariant theory. Chapters 14–19 present the fundamentals concerning pseudo-reflection groups and their rings of invariants. In particular, the cited Chevalley-Shephard-Todd-Bourbaki results are established. Chapters 20–26 are devoted to embellishments of the basic theory. Notably, skew invariants and the ring of covariants for pseudo-reflection groups are studied in some detail.

(III) Chapters 27–34: Conjugacy classes

The last eight chapters focus on the conjugacy classes of elements and subgroups in finite (pseudo) reflection groups. The first two parts of the book will have demonstrated that a great deal of information about (pseudo) reflection groups can be obtained from root systems and invariant theory, respectively. This third part continues this approach studying the conjugacy classes of (pseudo) reflection groups from the vantage point of either root systems or invariant theory. Chapters 27–30 are a continuation of Part I. They demonstrate how root systems can be used to provide information about canonical elements in Euclidean reflection groups, notably Coxeter elements and involutions. Chapters 31–34 are a continuation of Part II. These chapters study the eigenvalues and eigenspaces of elements in pseudo-reflection groups via the associated ring of invariants.

Reflection groups are not only of great interest in their own right. They also play a key role in other areas of mathematics. As already suggested, algebraic

groups, Lie theory, and the homology of classifying spaces, are areas where they particularly have found significant applications. In fact, the interest in reflection groups, and the drive to develop a full theory for them, arose precisely from their uses in these areas. Unfortunately, we shall only be able to hint at such connections in this book. Representative books for obtaining more information are: Benson [1], Carter [1], Humphrey [1] and Smith [1].

This book has evolved from various graduate courses given by the author over the past ten years at the University of Western Ontario. It is intended to be a graduate text, accessible to students with a sufficient background in algebra. The needs of the reader will vary from chapter to chapter. A basic knowledge of linear algebra, group theory, and ring theory is assumed. With this background, a great deal of the book is accessible. This is particularly true for the chapters dealing with Euclidean reflection groups. But certain chapters connected with invariant theory (notably 19, 25, 26, 33, 34) are more demanding of the reader, both with respect to background and to general mathematical maturity. Module theory and extension theory (Galois theory and its analogues in graded ring theory) is used throughout the study of invariant theory. A brief summary of graded ring and module theory is provided in Appendix A. It is useful, at times, to impose the framework of representation theory on reflection groups to better understand what is happening. Appendix B provides a short summary of the theory of group representations. Previous exposure to such background material as above is clearly a benefit. Quadratic forms are used in the classification of reflection groups and a summary of basic facts is provided in Appendix C. Other background is provided in short summaries at various places throughout the text. For example, graded extension theory is sketched in §16-3. As well, there is a summary of algebraic geometry in §33-2.

I Reflection groups

In Part I we introduce Euclidean reflection groups, and some of the more important concepts associated with their theory. The main theme of Part I is that the root systems associated with a given finite Euclidean reflection group can be used to analyze the group. In fact, most results are ultimately obtained by studying the canonical permutation action of reflection groups on their root system. Equivalently, from a geometrical point of view, we are looking at the configuration formed by the reflecting hyperplanes, and at the action of the reflection group on these hyperplanes. In Chapter 1, we define Euclidean reflection groups and discuss a number of important examples of such groups. In Chapter 2, we introduce root systems. A root system is a reformulation of a finite reflection group in terms of linear algebra. In Chapter 3, we introduce fundamental systems of root systems. In Chapter 4, we define the concept of length in a reflection group. In particular, we characterize length in terms of the action of the group on its root systems and prove the Matsumoto exchange and cancellation properties. In Chapter 5, we deal with parabolic subgroups. This last chapter is something of an appendix to the first four chapters of the book. It will not really be needed until the study of conjugacy classes in Chapters 27–30. However, the material is a natural extension of the discussion of fundamental systems, and so it is presented in Part I.

1 Euclidean reflection groups

The goal of this chapter is to introduce Euclidean reflection groups. This will be done in two ways. First of all, examples of reflection groups, in the plane and in 3-space, are discussed in detail. Secondly, we provide, via a preliminary discussion of Weyl chambers and invariant theory, a suggestion of the beautiful structure theorems that hold for reflection groups, and that explain the interest in such groups. The dihedral and symmetric groups will receive particular attention.

1-1 Reflections and reflection groups

We shall work in ℓ-dimensional *Euclidean space* $\mathbb{E}$. In other words, $\mathbb{E} = \mathbb{R}^\ell$ where $\mathbb{R}^\ell$ has the usual inner product. More abstractly, $\mathbb{E}$ is a ℓ-dimensional vector space over $\mathbb{R}$ provided with a pairing

$$(\_,\_)\colon \mathbb{E} \times \mathbb{E} \longrightarrow \mathbb{R}$$

satisfying:

(i) $(ax + by, z) = a(x,z) + b(y,z)$
(ii) $(x,y) = (y,x)$
(iii) $(x,x) \geq 0$ and $(x,x) = 0$ if and only if $x = 0$.

(In the above $x, y, z \in \mathbb{E}$, while $a, b \in \mathbb{R}$.)

We can define *reflections* either with respect to hyperplanes or vectors. First of all, given a hyperplane $H \subset \mathbb{E}$ through the origin, let $L =$ the line through the origin that is orthogonal to H. (So $\mathbb{E} = H \oplus L$.) Then, define the linear transformations $s_H\colon \mathbb{E} \longrightarrow \mathbb{E}$

$$s_H \cdot x = x \quad \text{if } x \in H$$
$$s_H \cdot x = -x \quad \text{if } x \in L.$$

We can also define reflections with respect to vectors. This is the formulation we shall be using. Given $0 \neq \alpha \in \mathbb{E}$, let $H_\alpha \subset \mathbb{E}$ be the hyperplane

$$H_\alpha = \{x \mid (x,\alpha) = 0\}.$$

We then define the reflection $s_\alpha\colon \mathbb{E} \longrightarrow \mathbb{E}$ by the rules

$$s_\alpha \cdot x = x \quad \text{if } x \in H_\alpha$$
$$s_\alpha \cdot \alpha = -\alpha.$$

Observe: Given $0 \neq k \in \mathbb{R}$, then $H_\alpha = H_{k\alpha}$ and $s_\alpha = s_{k\alpha}$.

We shall call H_α the *reflecting hyperplane* or *invariant hyperplane* of s_α. Here are some useful properties of s_α and H_α.

Properties:

(A-1) $s_\alpha \cdot x = x - \frac{2(x,\alpha)}{(\alpha,\alpha)}\alpha$ for all $x \in \mathbb{E}$
(A-2) s_α is *orthogonal*, i.e., $(s_\alpha \cdot x, s_\alpha \cdot y) = (x, y)$ for all $x, y \in \mathbb{E}$
(A-3) $\det s_\alpha = -1$
(A-4) If φ is an orthogonal automorphism of $\mathbb{E}$ then

$$\varphi \cdot H_\alpha = H_{\varphi\cdot\alpha}$$

$$\varphi s_\alpha \varphi^{-1} = s_{\varphi\cdot\alpha}.$$

To prove (A-1), check the effect of the RHS of the formula on H_α and on α. To prove (A-2), substitute formula (A-1) in $(s_\alpha \cdot x, s_\alpha \cdot y)$. To prove the first fact of (A-4), observe that $x \in H_\alpha$ implies $(\varphi \cdot x, \varphi \cdot \alpha) = (x, \alpha) = 0$. Hence, $\varphi \cdot H_\alpha \subset H_{\varphi\cdot\alpha}$. By comparing dimensions, we then have $\varphi \cdot H_\alpha = H_{\varphi\cdot\alpha}$. To prove the second fact of (A-4), check the effect of $\varphi s_\alpha \varphi^{-1}$ on $H_{\varphi\cdot\alpha} = \varphi \cdot H_\alpha$ and on $\varphi \cdot \alpha$.

Besides reflections, we also have the concept of a reflection group. Let

$$O(\mathbb{E}) = \{f\colon \mathbb{E} \to \mathbb{E} \text{ linear and } \big(f(\alpha), f(\beta)\big) = (\alpha, \beta) \text{ for all } \alpha, \beta\}$$

be the *orthogonal group* of $\mathbb{E}$. Given $W \subset O(\mathbb{E})$, we say that W is a Euclidean *reflection group* if W is generated, as a group, by its reflections. Two reflection groups $W \subset O(\mathbb{E})$ and $W' \subset O(\mathbb{E}')$ will be said to be *isomorphic* if there exists a linear isomorphism $f\colon \mathbb{E} \to \mathbb{E}'$ preserving inner products and conjugating W to W'. In other words,

$$\big(f(x), f(y)\big) = (x, y) \quad \text{for all } x, y \in \mathbb{E}$$

$$fWf^{-1} = W'.$$

A reflection group $W \subset O(\mathbb{E})$ is *reducible* if it can be decomposed as $W = W_1 \times W_2$, where both $W_1 \subset O(\mathbb{E})$ and $W_2 \subset O(\mathbb{E})$ are nontrivial subgroups generated by reflections from W. Otherwise a reflection group will be said to be *irreducible*. Our treatment of reflection groups will include a classification of those that are finite and irreducible.

The concept of a reflection as defined here can be generalized. Beginning in Chapter 14, we shall deal with *pseudo-reflections*, the extension of reflections to vector spaces over arbitrary fields. Our reason for beginning with Euclidean reflection groups is that they possess a theory all their own. In particular, we can use the trigonometry of the underlying Euclidean space to understand their structure. Section 1-4 provides a good illustration of this process.

Remark: We shall generally write our groups multiplicatively. The one exception to our multiplicative notation will be $\mathbb{Z}/n\mathbb{Z}$ for the cyclic group with n elements. Group actions on sets, $G \times S \to S$, are defined at the beginning of Appendix B. Such actions will be used extensively throughout this book. We use "$\cdot$" to denote group actions on a set. See properties (A-1), (A-2) and (A-4), above, for illustrations of this notation.

We finish this section with a key example of a reflection group.

Example: The Symmetric Group Σ_ℓ Σ_ℓ acts on $\mathbb{E} = \mathbb{R}^\ell = \{(x_1, \ldots, x_\ell)\}$ by permuting coordinates. We thereby obtain a subgroup $\Sigma_\ell \subset O(\mathbb{E})$. This subgroup is a reflection group. First of all, every permutation can be written as a product of the involutions $\{(i, j) \mid 1 \leq i < j \leq \ell\}$. Secondly, with the given action, these involutions are reflections on $\mathbb{R}^\ell$. For the involution $\tau = (i, j)$ fixes every element of the hyperplane

$$H_\tau = \{(x_1, \ldots, x_\ell) \mid x_i = x_j\}$$

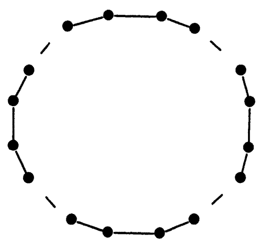
while it acts as -1 on the orthogonal line

$$L_\tau = \{(0, \ldots, 0, x_i, 0, \ldots, 0, x_j, 0, \ldots, 0) \mid x_i = -x_j\}.$$

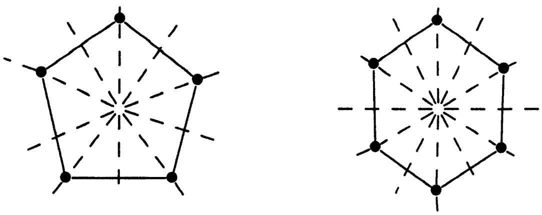
1-2 Groups of symmetries in the plane

In this section, we demonstrate that reflection groups occur quite naturally in the plane. Namely, when we consider the group of symmetries of certain planar objects, the groups turn out to have the additional property of being reflection groups. The next few sections will then be spent discussing these examples. The planar reflection groups will turn out to have a simple and elegant structure. They are *dihedral groups.* It will eventually be seen that these dihedral structures are indicative of the general situation. Every reflection group has a simple and elegant structure called a *Coxeter group presentation.* And dihedral groups turn out to be the simplest examples of such Coxeter group structures.

The automorphism group of the *n-gon* P_n



is a reflection group in the plane. The group consists of $2n$ elements. For if we pick a vertex on P_n, then any automorphism is determined by the image of the vertex plus the image of the two edges attached to it. The group consists of n rotations (forming a cyclic group of order n) plus n reflections. The following pictures illustrate the possible reflections for the case of the 5-gon and the 6-gon.



To see that the automorphism group of P_n is generated by its reflections, think of the plane as being divided into *chambers* via the n lines defining the reflections of the group. The picture above illustrates the process. Each chamber is a pie-shaped region touching the origin. Now, choose any chamber and consider the two reflections s_1, s_2 determined by its sides. These two reflections generate the group. First of all, $t = s_1 s_2$ is a rotation of order n (to see this, check the effect of t on the vertices of P_n). So $\{1, t, t^2, \dots, t^{n-1}\}$ are the n rotations. Secondly, $\{t^k s_1 t^{-k}\}$ for $0 \leq k \leq n-1$ are the reflections (to see this, check the effect of t^k on the vertices of P_n and then use rule (A-4) of §1-1).

We shall further analyze the above reflection groups in the next two sections. In §1-3 it will be shown that they are dihedral groups. Conversely, it will be shown in §1-4 that the examples of this section turn out to provide a complete list of planar reflection groups. The fact that planar reflection groups have a dihedral group structure, turns out to be the key to this classification. Chambers, and their relation to the structure of their associated reflection groups, will be further discussed in §1-6.

1-3 Dihedral groups

Before we define the dihedral group, we first recall what the semidirect product means. Recall that $H \subseteq K$ is *normal* if $kH = Hk$ for all $k \in K$, i.e., $kHk^{-1} = H$ for all $k \in K$. As usual, we use the notation $H \lhd K$ to denote a normal subgroup.

Definition: Given a group K with subgroups G and H satisfying

(i) $K = GH$, i.e., every element $k \in K$ can be written $k = gh$ where $g \in G$ and $h \in H$

(ii) $G \lhd K$

(iii) $G \cap H = \{1\}$

we then say that K is the *semidirect product* $G \rtimes H$.

Observe that the decomposition $k = gh$ in property (i) is unique. For if $g_1 h_1 = g_2 h_2$ then $g_1^{-1} g_2 = h_1 h_2^{-1}$. Since $G \cap H = \{1\}$, it follows that $g_1 = g_2$ and $h_1 = h_2$. This uniqueness property then tells us that $|K| = |G|\,|H|$.

Examples: Some of the symmetric groups are semidirect products. We can write

$$\Sigma_3 = \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z},$$

where $\mathbb{Z}/2\mathbb{Z}$ is generated by the involution $(1, 2)$ and $\mathbb{Z}/3\mathbb{Z}$ is generated by the cycle $(1, 2, 3)$. We can also write

$$\Sigma_4 = (\mathbb{Z}/2\mathbb{Z})^2 \rtimes \Sigma_3,$$

where $(\mathbb{Z}/2\mathbb{Z})^2$ is the Klein group $\{1, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$.

A semidirect product can also be specified by giving a group homomorphism $\phi\colon H \longrightarrow \mathrm{Aut}(G)$, where G and H are groups. (Here $\mathrm{Aut}(G)$ denotes the group

automorphisms of G. The group structure on $\mathrm{Aut}(G)$ is given by composition.) The semidirect product $G \rtimes H$ is the group whose underlying set is $G \times H$ and whose multiplication is defined by the rule

$$(g_1, h_1)(g_2, h_2) = \big(g_1[\phi(h_1)g_2], h_1h_2\big).$$

So the semidirect product multiplication is obtained by introducing a "twisting" factor $\phi(h_1)$ into the direct product multiplication. In particular, if ϕ is the trivial homomorphism (i.e., $\phi(h) = 1$ for all $h \in H$), then $G \rtimes H$ is the usual product $G \times H$ of the groups G and H.

We should also observe that, if G and H are considered subgroups of $G \rtimes H$, then the homomorphism $\phi\colon H \to \mathrm{Aut}(G)$ corresponds to the action of H on G as inner automorphisms.

Example: As an example of a semidirect product appearing often in this book consider $(\mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}) \rtimes \Sigma_\ell$, where we have ℓ copies of $\mathbb{Z}/2\mathbb{Z}$ and the symmetric group Σ_ℓ acts on $\mathbb{Z}/2\mathbb{Z}\times\cdots\times\mathbb{Z}/2\mathbb{Z}$ by permuting factors. The need for this semidirect product will quickly arise. The automorphism group of the cube (which will be discussed in §1-5) is the $\ell = 3$ case. The interest in $(\mathbb{Z}/2\mathbb{Z})^\ell \rtimes \Sigma_\ell$ lies in the fact that these groups are reflection groups. For there is a well-defined action of $(\mathbb{Z}/2\mathbb{Z})^\ell \rtimes \Sigma_\ell$ on $\mathbb{R}^\ell = \{(x_1, \ldots, x_\ell)\}$, given as follows:

Σ_ℓ permutes the coordinates $\{x_1, \ldots, x_\ell\}$

$(\mathbb{Z}/2\mathbb{Z})^\ell$ acts as sign changes on the coordinates $\{x_1, \ldots, x_\ell\}$.

As observed in §1-1, Σ_ℓ is a reflection group under the permutation action on $\mathbb{R}^\ell$. Similarly, $(\mathbb{Z}/2\mathbb{Z})^\ell$ is generated by reflections. For a sign change on a single factor is a reflection and these sign changes generate $(\mathbb{Z}/2\mathbb{Z})^\ell$. It follows that $(\mathbb{Z}/2\mathbb{Z})^\ell \rtimes \Sigma_\ell$ is an Euclidean reflection group.

We now introduce the dihedral group D_n.

Definition: The *dihedral group* is the group $D_n = \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ where if x generates $\mathbb{Z}/2\mathbb{Z}$ then $xyx = y^{-1}$ for any $y \in \mathbb{Z}/n\mathbb{Z}$.

Examples:

(a) $D_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
(b) $D_3 = \Sigma_3$. The identification $\Sigma_3 = \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ was made above.
(c) D_n = the automorphism group of P_n was discussed in §1-2. The dihedral structure $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ is obtained by letting x = any reflection of P_n and $\mathbb{Z}/n\mathbb{Z}$ = the rotations of P_n. We note that if y is chosen to be a generator of $\mathbb{Z}/n\mathbb{Z}$ (i.e., a rotation of order n), then the relations $x^2 = y^n = 1$ and $xyx = y^{-1}$ are all satisfied. This observation is relevant to Proposition A below.

By the discussion in §1-2, the dihedral groups can be represented as reflection groups in the plane. As we shall see in the next section, they are the only finite reflection groups in the plane.

We end this section with an alternative description of the dihedral group. By a presentation we mean a list of generators of the group plus a list of relations that hold between the generators. More formally, a *presentation of a group* will be written

$$G = \langle g_i \in G \mid r_1 = \cdots = r_n = 1 \rangle,$$

where $\{r_i\}$ are certain words in the elements $\{g_i\}$. The identity above means that $G = F/N$, where:

$$\begin{aligned} F &= \text{the free group generated by } \{g_i\}; \\ N &= \text{the normal subgroup of } F \text{ generated by the } \{r_i\} \\ &= \bigcap_{R \subset K \lhd F} K \text{ where } R = \{r_1, \ldots, r_n\}. \end{aligned}$$

In particular, F is the group consisting of all words that can be formed from the symbols $\{g_i\} \coprod \{g_i^{-1}\}$, subject only to the usual group relations e.g. $g_i g_i^{-1} = 1$. So F possesses as few relations as possible. Typically, presentations can be difficult to calculate. No such problems will arise in the case of dihedral groups. The next two propositions contain canonical presentations of the dihedral groups.

Write $D_n = \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ and let $x \in \mathbb{Z}/2\mathbb{Z}$ and $y \in \mathbb{Z}/n\mathbb{Z}$ be generators of the two subgroups. The dihedral group, then, has the following presentation.

Proposition A $D_n = \langle x, y \mid x^2 = y^n = (xy)^2 = 1 \rangle$.

Alternatively, let $s_1 = x$ and $s_2 = xy$. Then the presentation above can be reformulated as

Proposition B $D_n = \langle s_1, s_2 \mid (s_1)^2 = (s_2)^2 = (s_1 s_2)^n = 1 \rangle$.

From the viewpoint of reflection groups, this second formulation is the "correct" description of the dihedral group. It is the description arising for D_n when we interpret D_n as the automorphism group of the n-gon P_n and, hence, as a reflection group in the plane. Namely, if we return to our previous discussion in §1-2, where we established that the automorphism group of P_n is a reflection group, then s_1 and s_2 can be chosen as the two generating reflections obtained from the walls of any chamber. In Chapter 6 we shall generalize the concept of a dihedral group to that of a Coxeter group. A Coxeter group has a special type of presentation that is analogous to, but more general than, the dihedral group presentation given in Proposition B. As in the special case of the dihedral group, the Coxeter group structure is closely related to the geometry of the reflection group. Conversely, an arbitrary finite reflection group can be characterized by such Coxeter group structures.

We are left with verifying Propositions A and B. Since the propositions are equivalent, we shall prove Proposition B.

Proof of Proposition B We have a well-defined surjective map $F(s_1, s_2)/N \to D_n$. Moreover, by a counting argument, it is an isomorphism. We know $|D_n| = 2n$, but also $|F/N| = 2n$. To obtain this second identity, we use the relations $(s_1)^2 = (s_2)^2 = 1$ to reduce the words of F/N to the form $s_1s_2s_1s_2\cdots$ or $s_2s_1s_2s_1\cdots$. The relations $(s_1s_2)^n = (s_2s_1)^n = 1$ can then be used to reduce further the words of F/N to expressions $s_1s_2s_1s_2\cdots$ or $s_2s_1s_2s_1\cdots$, where no more than n terms are involved. For example, if $(s_1s_2)^3 = 1$, then $s_1s_2s_1s_2 = s_2s_1$. We have now reduced the number of words in F/N to at most $2n$. ■

1-4 Planar reflection groups as dihedral groups

In this section, we finish our discussion of finite reflection groups in the plane. In §1-3 we showed that dihedral groups are planar reflection groups. In these sections we show that every finite reflection group in the plane is a dihedral group. We shall actually show more. As already observed, every reflection is an orthogonal transformation. We shall show the following.

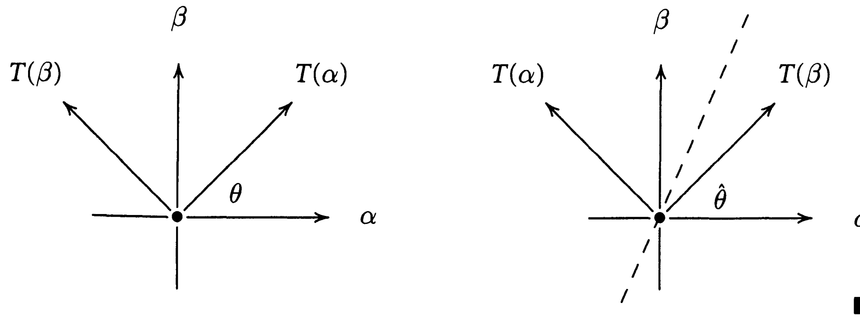
Theorem

(i) Every orthogonal transformation of the plane is either a reflection or a rotation.
(ii) The only finite subgroups of the orthogonal group $O(\mathbb{R}^2)$ *are the cyclic groups,* $\mathbb{Z}/n\mathbb{Z}$*, consisting of rotations and the dihedral groups,* D_n*, generated by reflections.*

The following lemma tells us which of the orthogonal transformations of the plane are reflections.

Lemma A *Every orthogonal transformation of the Euclidean plane is a reflection* (det $= -1$) *or a rotation* (det $= 1$).

Proof We consider the effect of an orthogonal transformation T on the two vectors $\alpha = (1, 0)$ and $\beta = (0, 1)$. The orthogonality of T forces $T(\alpha)$ and $T(\beta)$ to also be of unit length and orthogonal to each other. Let θ and $\hat{\theta}$ be the counterclockwise angles formed by $T(\alpha)$ and $T(\beta)$ with the x-axis. Then $\hat{\theta} = \theta \pm \pi/2$. In the case $\hat{\theta} = \theta + \pi/2$, T is a rotation through angle θ. In the case $\hat{\theta} = \theta - \pi/2$, T is a reflection through the dashed line forming an angle of $\theta/2$ with the x-axis. In pictures we have



■

We now set about using Lemma A to determine the finite subgroups of $O(\mathbb{R}^2)$. *Suppose $G \subset O(\mathbb{R}^2)$ is a finite subgroup.* By Lemma A, we know that every element of G is either a reflection or a rotation. Moreover, the rotations of G form the subgroup $\mathrm{Ker}\{\det\colon G \to \{\pm 1\}\}$. So the rotation subgroup either equals G, or is of index 2.

Lemma B *The rotation subgroup is of the form $\mathbb{Z}/n\mathbb{Z}$ for some n.*

Proof Choose a (counterclockwise) rotation T with $\theta(T)$ (= angle of rotation) minimal. Pick an arbitrary rotation $S \in G$. We want to show $S = T^k$ for some integer k. Pick the integer k such that $k\theta(T) \leq \theta(S) < (k+1)\theta(T)$, i.e.,

$$0 \leq \theta(S) - k\theta(T) < \theta(T).$$

Now ST^{-k} is a rotation through $\theta(S) - k\theta(T)$. So the minimality of $\theta(T)$ forces $\theta(S) - k\theta(T) = 0$. The identity $\theta(S) = k\theta(T)$ then forces $S = T^k$. ■

Lemma C *If G contains reflections, then G is the reflection group D_n for some n.*

Proof First of all, G is a dihedral group. Let $\mathbb{Z}/n\mathbb{Z} \subset G$ be the rotation subgroup. By previous comments, $\mathbb{Z}/n\mathbb{Z} \subset G$ must have index 2 (i.e., $|G| = 2n$). Choose a reflection R, plus a rotation T generating $\mathbb{Z}/n\mathbb{Z}$. We have the relations

$$R^2 = T^n = 1 \quad \text{and} \quad RTR = T^{-1}.$$

Regarding the last relation, observe that RT is a reflection, since

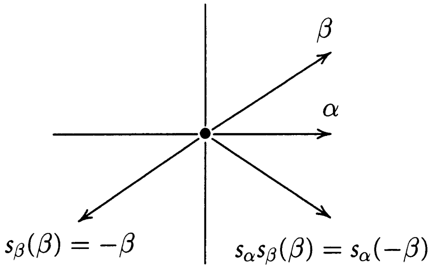
$$\det(RT) = \det(R)\det(T) = (-1)(1) = -1.$$

So $RTRT = (RT)^2 = 1$ and $RTR = T^{-1}$. This observation also establishes that G is a reflection group. For, since $(R)(RT) = T$, it follows that R and RT generate G. ■

The next lemma, at the moment, is only an aside. But it will later play an important role. It demonstrates that the algebra of a finite reflection group reflects its geometry. See §1-6 for an indication of its usefulness.

Lemma D *Given $\alpha, \beta \in \mathbb{R}^2$, then $s_\alpha s_\beta$ is a rotation through twice the angle between α and β.*

Proof $\det(s_\alpha s_\beta) = \det(s_\alpha)\det(s_\beta) = (-1)(-1) = 1$. So, by Lemma A, $s_\alpha s_\beta$ is a rotation through some angle. To determine the angle, determine the effect of $s_\alpha s_\beta$ on β. The following picture illustrates that β is moved (in this case, clockwise) through twice the angle between α and β.



Remark: The above lemma actually holds in arbitrary dimensions. For, given $\alpha, \beta \in \mathbb{R}^\ell$, we can write $\mathbb{R}^\ell = A \oplus B$, where

$$A = H_\alpha \cap H_\beta \quad \text{and} \quad B = \mathbb{R}\alpha + \mathbb{R}\beta.$$

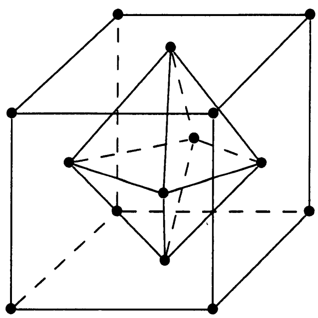
Then, by property (A-1) of §1-1, s_α and s_β respect the decomposition: they map B to itself and leave A pointwise invariant. So we can reduce to the subspace B, in which case Lemma D can be applied.

1-5 Groups of symmetries in 3-space

We now turn to the automorphism groups of certain three-dimensional figures that will turn out to be reflection groups in 3-space. Unlike the planar reflection groups, the three-dimensional groups are reasonably complicated and tend to illustrate that reflection groups are difficult to analyze, and that some general structure theorems are needed in order to see what is going on.

We shall consider the automorphism groups of the five Platonic solids: tetrahedron, cube, octahedron, dodecahedron and icosahedron (displayed in Figure 1).

We always think of the Platonic solids as embedded in 3-space with their centroid at the origin. Thus the automorphisms of each solid can be regarded as orthogonal transformations of $\mathbb{R}^3$. Actually, there are only three automorphism groups to consider. The automorphism groups of the cube and octahedron coincide, as do those of the icosahedron and dodecahedron. For example, the octahedron can be imbedded in the cube in the following fashion.



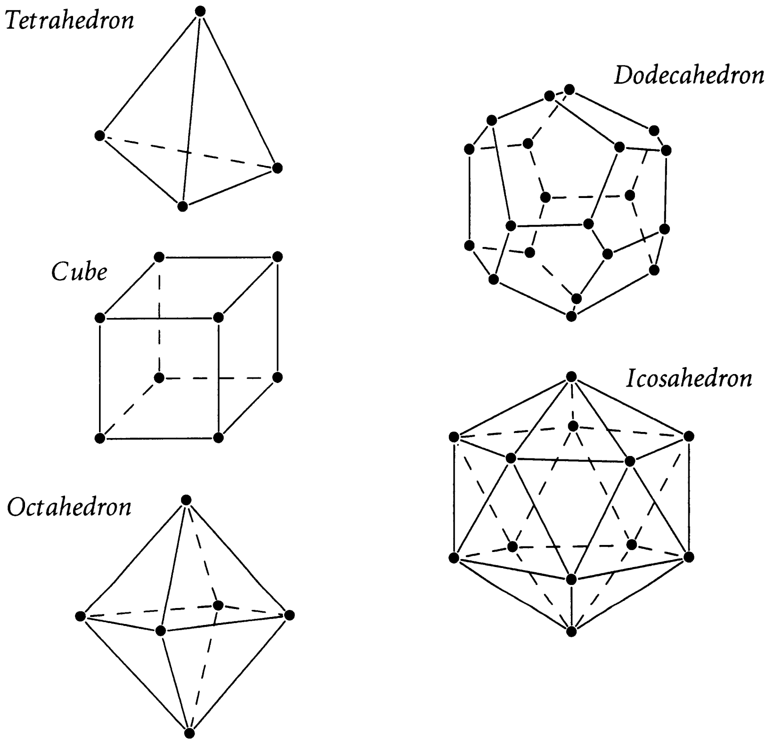


Figure 1: The Platonic solids

So any automorphism of the cube induces an automorphism of the octahedron, and vice versa. Similarly, there is an imbedding of the dodecahedron in the icosahedron that gives a correspondence between their transformation groups.

We now give brief summaries of the automorphism groups of the Platonic solids. For further details on the Platonic solids and their automorphisms, consult Rees [1].

(a) Tetrahedron

The automorphism group of the tetrahedron is the permutation group Σ_4; for an automorphism of the tetrahedron is determined by its effect on the four vertices of the tetrahedron. Moreover, all permutations of these vertices are possible.

The tetrahedron admits 6 reflections. They can be identified with the switching of any two vertices and, hence, with the involutions $\{(i,j) \mid 1 \leq i < j \leq 4\}$ of Σ_4. These involutions generate Σ_4. So the tetrahedron automorphism group is a reflection group.

(b) Cube

The automorphism group of the cube consists of 48 elements; for an automorphism of the cube is determined by the image of a vertex and the three edges attached to it. Thus there are $(8)(3!) = 48$ possibilities. It is easy to locate two sets of automorphisms that, when combined, produce all 48 of these possibilities. Let Σ_3 be the permutations of the edges attached to a given vertex α, and let $(\mathbb{Z}/2\mathbb{Z})^3$ be the subgroup generated by the three reflections whose reflecting planes bisect the cube and are parallel to a face. (Observe that these three planes are orthogonal to each other and, hence, the associated reflections commute with each other.) The elements of $(\mathbb{Z}/2\mathbb{Z})^3$ can be used to move the given vertex α onto any of the eight vertices of the cube.

By the above remarks, every automorphism of the cube can be decomposed into a product of elements from Σ_3 and $(\mathbb{Z}/2\mathbb{Z})^3$. Notice, however, that the automorphism group of the cube is not the direct product $\Sigma_3 \times (\mathbb{Z}/2\mathbb{Z})^3$; for the elements of Σ_3 and of $(\mathbb{Z}/2\mathbb{Z})^3$ do not typically commute with each other. The automorphism group of the cube is actually a semidirect product $(\mathbb{Z}/2\mathbb{Z})^3 \rtimes \Sigma_3$. The permutation action of Σ_3 on $(\mathbb{Z}/2\mathbb{Z})^3$ gives the homomorphism $\phi\colon \Sigma_3 \to \mathrm{Aut}\big((\mathbb{Z}/2\mathbb{Z})^3\big)$ used to construct the semidirect product.

This automorphism group is a reflection group. By definition, the factor $(\mathbb{Z}/2\mathbb{Z})^3$ is generated by reflections. The same is also true of the factor Σ_3; for Σ_3 is generated by any two of its involutions. Each involution fixes one of the edges attached to α and switches the other two. So each involution is a reflection.

The cube admits a total of nine reflections. There are the three reflections which generate $(\mathbb{Z}/2\mathbb{Z})^3$. Six other reflecting planes are determined by using the six pairs of opposite edges of the cube.

We notice that the automorphism group can be written as $\Sigma_4 \times \mathbb{Z}/2\mathbb{Z}$. Here Σ_4 permutes the four diagonal axes of the cube, while $\mathbb{Z}/2\mathbb{Z}$ is given by the antipodal map. The equivalence of the two descriptions, $\Sigma_4 \times \mathbb{Z}/2\mathbb{Z}$ and $(\mathbb{Z}/2\mathbb{Z})^3 \rtimes \Sigma_3$, can also be deduced from the identity $\Sigma_4 = (\mathbb{Z}/2\mathbb{Z})^2 \rtimes \Sigma_3$ of §1-3.

(c) Dodecahedron

The automorphism group of the dodecahedron can be identified with the group $A_5 \times \mathbb{Z}/2\mathbb{Z}$, where $A_5 \subset \Sigma_5$ is the alternating group. Observe, first of all, that an automorphism of the dodecahedron is determined by the image of any vertex, and of the three edges attached to it. Since there are 20 vertices, there are $(20)(3!) = 120$ possibilities. The subgroup A_5 is given as permutations on five imbedded tetrahedrons, while $\mathbb{Z}/2\mathbb{Z}$ comes from the antipodal map. To locate the five tetrahedrons, label each vertex of the icosahedron by one of the integers $\{1, 2, 3, 4, 5\}$ and do so in such a fashion that the five vertices of each face (which is a pentagon) have the complete set. (We start by labelling one of the pentagonal faces, and move outwards.) We then have four vertices labelled by each of $1, 2, 3, 4, 5$. The four vertices labelled by any of these integers determine a tetrahedron.

The dodecahedron has fifteen reflections, each reflection plane being determined by a pair of opposite edges. It follows from property (A-4) of §1-1 that these reflections are permuted among themselves under conjugation. Consequently, the subgroup H generated by the reflections is a normal subgroup of $\mathbb{Z}/2\mathbb{Z} \times A_5$. But A_5 is a simple group. So the only possibilities for H are $H = \mathbb{Z}/2\mathbb{Z}$, A_5, or $\mathbb{Z}/2\mathbb{Z} \times A_5$. Since H contains fifteen distinct reflections, we can eliminate $H = \mathbb{Z}/2\mathbb{Z}$. We can also eliminate $H = A_5$. The group A_5 does contain fifteen involutions. However, as automorphisms of the dodecahedron, these fifteen involutions are rotations through the angle π about the line determined by the midpoints of any two opposite edges, so they are not reflections. We are left with $H = \mathbb{Z}/2\mathbb{Z} \times A_5$ as the only possibility.

Remark: As a suggestion of the subtle structure of a reflection group, we point out that, for dihedral groups as well as for the examples above, the number of reflections in the group is related to the order of the group. In the case of the automorphism group of the n-gon, the integers $d_1 = 2$ and $d_2 = n$ satisfy the relations that the order of the group is $d_1 d_2$, while the number of reflections is $(d_1 - 1) + (d_2 - 1)$. In the case of the automorphism groups of the tetrahedron, cube and dodecahedron, we can find integers $\{d_1, d_2, d_3\}$ so that the order of the group is $d_1 d_2 d_3$, while the number of reflections is $(d_1 - 1) + (d_2 - 1) + (d_3 - 1)$. We let $\{d_1, d_2, d_3\}$ be $\{2, 3, 4\}$, $\{2, 4, 6\}$ and $\{2, 6, 10\}$ respectively. The integers $\{d_1, d_2\}$ or $\{d_1, d_2, d_3\}$ are called the *degrees* of the group. They arise in the invariant theory of reflection groups. A brief introduction to invariant theory and to degrees is given in §1-7. A complete discussion and explanation of the relation above is given in Chapter 18.

A great deal of work has to be done in order to prove the results outlined in the preceding paragraph. These assertions are really advertisements for the need for general structure theorems in order to understand precisely what is going on. These general structure theorems will be provided in Chapters 4 and 6.

Such additional structure theorems, as well as techniques for the analysis of reflection groups in arbitrary dimensions, will be suggested in §1-6 and §1-7. In §1-6 we shall discuss chambers, and show how they can be used to analyze reflec-

tion groups. In §1-7 invariant theory is introduced, and the key role played in that theory by reflection groups is suggested.

The automorphism groups of both the tetrahedron and the cube are part of a general pattern. Namely, for each $\ell \geq 3$, we can consider the automorphism groups of the ℓ-simplex and of the ℓ-cube, and show that they form systematic families of Euclidean reflection groups. Only the automorphism group of the dodecahedron is an "exceptional" reflection group, i.e., not part of an infinite family. Below, $\{\epsilon_1, \epsilon_2, \ldots, \epsilon_\ell\}$ will denote an orthonormal basis of the relevant Euclidean space $\mathbb{E} = \mathbb{R}^\ell$.

(a) Symmetry Group of the ℓ-Cube

If we imbed the ℓ-cube I^ℓ in $\mathbb{R}^\ell$ by the rule

$$I^\ell = \left\{ \sum_{i=1}^{\ell} c_i \epsilon_i \;\middle|\; -1 \leq c_i \leq +1 \right\},$$

then the symmetries of I^ℓ form the group $(\mathbb{Z}/2\mathbb{Z})^\ell \rtimes \Sigma_\ell$, where Σ_ℓ permutes $\{\epsilon_1, \epsilon_2, \ldots, \epsilon_\ell\}$, while $(\mathbb{Z}/2\mathbb{Z})^\ell$ acts as sign changes on $\{\epsilon_1, \epsilon_2, \ldots, \epsilon_\ell\}$. If we consider $(\mathbb{Z}/2\mathbb{Z})^\ell \rtimes \Sigma_\ell$ as acting on all of $\mathbb{R}^\ell$ (not just on $I^\ell \subset \mathbb{R}^\ell$) by the same recipe, then we have the reflection group $(\mathbb{Z}/2\mathbb{Z})^\ell \rtimes \Sigma_\ell$ described in §1-3.

(b) Symmetry Group of the ℓ-Simplex

We can imbed the ℓ-simplex Δ_ℓ in $\mathbb{R}^{\ell+1}$ by the rule

$$\Delta_\ell = \left\{ \sum_{i=1}^{\ell+1} c_i \epsilon_i \;\middle|\; c_i \geq 0 \text{ and } \sum_{i=1}^{\ell+1} c_i = 1 \right\}.$$

The symmetry group of this ℓ-simplex is $\Sigma_{\ell+1}$; for the vertices of Δ_ℓ are the points $\{\epsilon_1, \epsilon_2, \ldots, \epsilon_{\ell+1}\}$, and the symmetries of Δ_ℓ are obtained by permuting these vertices.

We observed in §1-2 that the permutation action of $\Sigma_{\ell+1}$ on the factors of $\mathbb{R}^{\ell+1}$ gives a reflection group structure. This reflection group action permutes the elements $\{\epsilon_1, \epsilon_2, \ldots, \epsilon_{\ell+1}\}$, and is clearly an extension of the action of $\Sigma_{\ell+1}$ on Δ_ℓ. Thus the symmetries of the ℓ-simplex can naturally be identified as a reflection group.

1-6 Weyl chambers

We have finished discussing reflection groups in the plane and in 3-space. We now turn to the question of analyzing reflection groups in Euclidean space of arbitrary dimension. In this section we indicate how to study such groups by their associated geometry. We shall give a preliminary indication of how the algebra and geometry of a finite Euclidean reflection group are related, and how to use this relation to analyze the group.

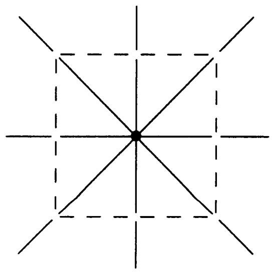
By *geometry* we mean the configuration formed by the reflection hyperplanes of the group. We want to understand how the hyperplanes relate to each other, i.e., we want to determine the geometrical figures formed by the intersecting hyperplanes.

The most important (and therefore useful) figure we can form from the hyperplanes is that of a chamber. As in §1-1, for any $\alpha \in \mathbb{E} = \mathbb{R}^\ell$, H_α denotes the hyperplane $H_\alpha = \{t \mid (t, \alpha) = 0\}$. Each H_α partitions $\mathbb{E}$, namely $\mathbb{E} - H_\alpha$ decomposes into two disjoint connected components

$$\mathbb{E}^+_\alpha = \{t \mid (\alpha, t) > 0\}$$
$$\mathbb{E}^-_\alpha = \{t \mid (\alpha, t) < 0\}.$$

Let $\{H_\alpha\}$ be the reflecting hyperplanes of a finite Euclidean reflection group $W \subset O(\mathbb{E})$. A *(Weyl) chamber* of W is a connected component of $\mathbb{E} - (\bigcup_\alpha H_\alpha)$. Given t and t' in $\mathbb{E} - (\bigcup_\alpha H_\alpha)$, then t and t' are in the same chamber if and only if they are on "the same side" of each hyperplane H_α. In other words, (t, α) and (t', α) must have the same sign for each α. A chamber of $\mathbb{E}$ is not a subspace, but it is closed under addition and scalar multiplication by positive scalars. We note that chambers always exist, i.e., $\mathbb{E} \neq \bigcup_\alpha H_\alpha$ and, so, $\mathbb{E} - (\bigcup_\alpha H_\alpha)$ has, at least, one nontrivial component. We defer the proof of this until §3-3.

The following picture illustrates two dimensional chambers.



Here we are dealing with the dihedral group D_4 = the automorphism group of the square (see the dashed lines). The solid lines are the axes of reflection for the various reflections of D_4. The eight pie-shaped regions between the solid lines are the chambers.

As we shall discover in the next few chapters, the hyperplanes and their associated Weyl chambers can give an enormous amount of information about the algebraic structure of a reflection group. A reflection group W permutes its reflecting hyperplanes (see property (A-4) of §1-1). This permutation action induces an action of W on its chambers. The action of W on its hyperplanes and chambers is closely related to the algebraic structure of W and is very useful for analyzing it. We close this section by using reflection groups in the plane and 3-space to provide two indications of this fact.

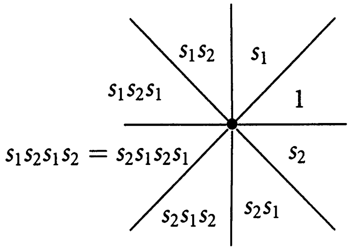
Example 1: As the first illustration of the relation between a reflection group and its chambers, let us consider (again) the Weyl chambers of the dihedral group D_4.

We know that

$$D_4 = \langle s_1, s_2 \mid (s_1)^2 = (s_2)^2 = (s_1 s_2)^4 = 1 \rangle.$$

This presentation can be read from the chamber diagram of D_4. How do we find generators of D_4? We choose any chamber and take the reflections in the two hyperplanes bounding the chamber (see §1-2). How do we find the relations between the generators? The relations $(s_1)^2 = (s_2)^2 = 1$ follow from the fact that we have chosen reflections. The relation $(s_1 s_2)^4 = 1$ follows from the fact that the angle between the lines forming the chamber (which are also the reflecting lines associated to the reflections s_1 and s_2) is $\pi/4$ (see Lemma D of §1-4).

So the basic algebraic structure of D_4 is related to the geometry of its Weyl chambers. But there are even more sophisticated relations between D_4 and the chambers. These relations are obtained by considering the action of D_4 on its chambers. Consider the following embellishment of the Weyl chamber diagram of D_4.



Here 1 denotes the designated chamber chosen above, whereas s_1 and s_2 again denote the reflections in the lines bounding that chamber. Then D_4 acts transitively on the chambers. We have labelled each chamber by the element of D_4, which sends the canonical chamber to it. The above labelling is related to the structure of D_4. First of all, there is a one-to-one correspondence between the elements of D_4 and the chambers; for it is easy to see that the elements of D_4 appearing in the picture are all the elements of D_4. Secondly, if we take any element of D_4, then the number of hyperplanes separating its chamber from the canonical chamber is equal to the minimal number of copies of s_1 and s_2 required to form the element.

Example 2: The transformation groups of the tetrahedron, cube (or octahedron), and dodecahedron (or icosahedron) possess presentations analogous to that obtained in Proposition 1-3 for the dihedral group. This is much harder to see than in our two-dimensional example. However, the general principle of analyzing these three-dimensional groups is still similar to that used for the two-dimensional groups. We take all the reflections in the group and use their associated reflecting planes to divide $\mathbb{R}^3$ into chambers. Each chamber has three walls. Choose any chamber and the three reflections associated with its walls. These generate the group. If we work out the relations between these generators, then we can obtain the following presentations of the three automorphism groups.

(a) Tetrahedron

$$\langle s_1, s_2, s_3 \mid (s_1)^2 = (s_2)^2 = (s_3)^2 = (s_1 s_3)^2 = (s_1 s_2)^3 = (s_2 s_3)^3 = 1 \rangle.$$

(b) Cube

$$\langle s_1, s_2, s_3 \mid (s_1)^2 = (s_2)^2 = (s_3)^2 = (s_1s_3)^2 = (s_1s_2)^3 = (s_2s_3)^4 = 1\rangle.$$

(c) Dodecahedron

$$\langle s_1, s_2, s_3 \mid (s_1)^2 = (s_2)^2 = (s_3)^2 = (s_1s_3)^2 = (s_1s_2)^3 = (s_2s_3)^5 = 1\rangle.$$

Thus the three groups are distinguished by the single relation $(s_2s_3)^m = 1$.

As we study Euclidean reflection groups, we shall see that both of the above examples are part of general patterns. Moreover, understanding these patterns for arbitrary reflection groups is the key to understanding the reflection groups themselves. The general structure theorems will be provided in Chapters 4 and 6.

1-7 Invariant theory

The material in this concluding section is meant to provide another perspective on the appeal and importance of reflection groups. It briefly introduces invariant theory, and suggests the special role that reflection groups play in that theory. This section is only a preliminary treatment of this fascinating subject. Invariant theory is treated in much more detail later in the book. In particular, the type of relations suggested here will be fully analyzed and justified in Chapters 16 through 18. Let P denote the ring of polynomial functions on $\mathbb{E} = \mathbb{R}^\ell = \{(x_1, \dots, x_\ell)\}$. We can write

$$P = \mathbb{R}[t_1, \dots, t_\ell],$$

where $t_i \colon \mathbb{R}^\ell \to \mathbb{R}$ denotes the linear functional $t_i(x_1, \dots, x_\ell) = x_i$. Given a subgroup $G \subset O(\mathbb{E})$, then the action of G on $\mathbb{E}$ induces an action on P by the rule

$$\varphi \cdot f(x) = f(\varphi^{-1} \cdot x).$$

We can then consider the subring $P^G \subset P$ of *invariant polynomials*, i.e.,

$$P^G = \{f \in P \mid \varphi \cdot f = f \text{ for all } \varphi \in G\}.$$

The outstanding problem of invariant theory is to understand the ring structure of P^G for various G and, more comprehensively, to understand the relation between that structure and the group structure of G. In the case of finite reflection groups, the answers turn out to be very elegant and informative. The second part of this book will be devoted to exploring the beautiful relations between (pseudo) reflection groups and their invariant theory. In this current section, we limit ourselves to providing some concrete examples of rings of invariant polynomials.

All our examples are connected with the symmetric group Σ_ℓ, but the examples will be indicative of the general situation. In what follows, we shall always write $\mathbb{R}^\ell = \{(x_1, \dots, x_\ell)\}$, and let $\{t_1, \dots, t_\ell\}$ be the projections defined above. Given a reflection group $W \subset O(\mathbb{E})$, then its ring of invariant polynomials $\mathbb{R}[t_1, \dots, t_\ell]^W$ always forms a *polynomial algebra*, i.e., there exist W invariant

homogeneous polynomials $\{f_1, \ldots, f_\ell\}$ such that every W invariant polynomial can be written uniquely as an algebraic expression in $\{f_1, \ldots, f_\ell\}$. In other words, every invariant polynomial is a unique polynomial in $\{f_1, \ldots, f_\ell\}$. We shall adopt the following polynomial algebra notation to describe this situation.

$$\mathbb{R}[t_1, \ldots, t_\ell]^W = \mathbb{R}[f_1, \ldots, f_\ell].$$

Example 1: $G = \Sigma_3$.

Before dealing with the general symmetric group, we first consider a particular case. The symmetric group Σ_3 is a reflection group when it acts on 3-space $\mathbb{E} = \mathbb{R}^3 = \{(x_1, x_2, x_3)\}$ by permuting coordinates. Moreover, the invariant polynomials of $\Sigma_3 \subset O(\mathbb{E})$ have a very simple pattern. First of all, Σ_ℓ acts on the polynomial ring $P = \mathbb{R}[t_1, t_2, t_3]$ by permuting the terms $\{t_1, t_2, t_3\}$. The polynomials

$$\begin{aligned} s_1 &= t_1 + t_2 + t_3 \\ s_2 &= t_1t_2 + t_2t_3 + t_1t_3 \\ s_3 &= t_1t_2t_3 \end{aligned}$$

are fixed under this action. And every polynomial that is invariant under permutations of $\{t_1, t_2, t_3\}$ can be written uniquely as a polynomial in $\{s_1, s_2, s_3\}$ (see Lang [1]). For example, the invariant polynomials $f = t_1^2 + t_2^2 + t_3^2$ and $g = t_1^3 + t_2^3 + t_3^3$ can be written

$$\begin{aligned} f &= s_1^2 - 2s_2 \\ g &= s_1^3 - 3s_1s_2 - 3s_3. \end{aligned}$$

We describe the algebraic structure of P^{Σ_3} as a polynomial algebra in $\{s_1, s_2, s_3\}$:

$$P^{\Sigma_3} = \mathbb{R}[t_1, t_2, t_3]^{\Sigma_3} = \mathbb{R}[s_1, s_2, s_3].$$

Example 2: The Symmetric Group Σ_ℓ The symmetric group Σ_ℓ is a reflection group when it acts on $\mathbb{E} = \mathbb{R}^\ell = \{(x_1, \ldots, x_\ell)\}$ by permuting coordinates. This permutation action induces an action on the polynomial ring $P = \mathbb{R}[t_1, \ldots, t_\ell]$, where Σ_ℓ permutes $\{t_1, \ldots, t_\ell\}$ in the canonical fashion. There are some standard polynomials that are fixed by this action, namely the k-th *elementary symmetric polynomial*

$$s_k = \sum_{1 \leq i_1 < \cdots < i_k \leq \ell} t_{i_1} \cdots t_{i_k} = \text{the coefficient of } T^{\ell-k} \text{ in } \prod_{i=1}^{k} (T + t_i).$$

Every polynomial fixed by Σ_ℓ can be constructed from $\{s_1, \ldots, s_\ell\}$. More exactly, and analogously to Example 1, every polynomial invariant under permutations of $\{t_1, \ldots, t_\ell\}$ can be written uniquely as a polynomial in $\{s_1, \ldots, s_\ell\}$, i.e.,

$$P^{\Sigma_\ell} = \mathbb{R}[t_1, \ldots, t_\ell]^{\Sigma_\ell} = \mathbb{R}[s_1, \ldots, s_\ell]$$

(see Lang [1]).

Example 3: The Reflection Group $(\mathbb{Z}/2\mathbb{Z})^\ell \rtimes \Sigma_\ell$ As observed in §1-3, $(\mathbb{Z}/2\mathbb{Z})^\ell \rtimes \Sigma_\ell$ is a reflection group when it acts on $\mathbb{E} = \mathbb{R}^\ell = \{(x_1, \ldots, x_\ell)\}$ by permuting coordinates (via Σ_ℓ) and changing their signs (via $(\mathbb{Z}/2\mathbb{Z})^\ell$). The induced action of $(\mathbb{Z}/2\mathbb{Z})^\ell \rtimes \Sigma_\ell$ on $P = \mathbb{R}[t_1, \ldots, t_\ell]$ is of the same type: the terms $\{t_1, \ldots, t_\ell\}$ are permuted and sign changes are induced. This action extends the one in Example 2 for Σ_ℓ, and the invariant polynomials of $(\mathbb{Z}/2\mathbb{Z})^\ell \rtimes \Sigma_\ell$ also turn out to be a variation of those for Σ_ℓ. Namely,

$$P^{(\mathbb{Z}/2\mathbb{Z})^\ell \rtimes \Sigma_\ell} = \mathbb{R}[t_1, \ldots, t_\ell]^{(\mathbb{Z}/2\mathbb{Z})^\ell \rtimes \Sigma_\ell} = \mathbb{R}[\bar{s}_1, \ldots, \bar{s}_\ell],$$

where $\bar{s}_k$ is obtained from s_k by replacing each t_i by t_i^2, i.e.,

$$\bar{s}_k = \sum_{1 \le i_1 < \cdots < i_k \le \ell} t_{i_1}^2 \cdots t_{i_k}^2.$$

Degrees When writing $\mathbb{R}[t_1, \ldots, t_\ell]^W = \mathbb{R}[f_1, \ldots, f_\ell]$ the choice of the homogeneous polynomials $\{f_1, \ldots, f_\ell\}$ is far from unique. Notably, we can always alter a given choice by decomposable elements. However, their degrees $\{d_1, \ldots, d_\ell\}$ are independent of any such choices. The degrees only depend on the reflection group in question, and are called the *degrees of the reflection group.* These integers have already been introduced. They are the integers referred to during the discussion of the automorphism groups of the Platonic solids in §1-5. They have the property that $|W| = d_1 \cdots d_\ell$, while $(d_1 - 1) + \cdots + (d_\ell - 1) =$ the number of reflections in W. The degrees of the symmetric group $\Sigma_\ell \subset O(\mathbb{R}^\ell)$, and of the cubical group $(\mathbb{Z}/2\mathbb{Z})^\ell \rtimes \Sigma_\ell \subset O(\mathbb{R}^\ell)$, were determined above. They provide more fully realized examples of this property. The polynomials $\{s_1, \ldots, s_\ell\}$ have degrees $\{1, 2, \ldots, \ell\}$, while the polynomials $\{\bar{s}_1, \ldots, \bar{s}_\ell\}$ have degrees $\{2, 4, \ldots, 2\ell\}$. We have the identities

$$|\Sigma_\ell| = \ell!$$
$$|\Sigma_\ell \rtimes (\mathbb{Z}/2\mathbb{Z})^\ell| = 2^\ell(\ell!),$$

which are examples of the property $|W| = d_1 \cdots d_\ell$. And we have the identities

$$\#\text{ of reflections in } \Sigma_\ell = \frac{\ell(\ell-1)}{2}$$
$$\#\text{ of reflections in } (\mathbb{Z}/2\mathbb{Z})^\ell \rtimes \Sigma_\ell = \ell^2,$$

which agrees with the rule that the number of reflections in W should be $(d_1 - 1) + \cdots + (d_\ell - 1)$. Regarding these last identities, observe that the reflections of Σ_ℓ consist of the involutions $\{(i, j) \mid 1 \le i < j \le \ell\}$ and, so, there

are $\frac{\ell(\ell-1)}{2}$ of them. The involution (i, j) exchanges the coordinates x_i and x_j. In the case of $(\mathbb{Z}/2\mathbb{Z})^\ell \rtimes \Sigma_\ell$, besides the reflections above, we can also obtain $\frac{\ell(\ell-1)}{2}$ reflections by combining each involution (i, j) with sign changes on the coordinates x_i and x_j. As well, there are ℓ reflections coming from the sign changes on a single coordinate. So there are $\frac{\ell(\ell-1)}{2} + \frac{\ell(\ell-1)}{2} + \ell = \ell^2$ reflections in $(\mathbb{Z}/2\mathbb{Z})^\ell \rtimes \Sigma_\ell$.

2 Root systems

A root system is a reformulation, in terms of linear algebra, of the concept of a finite Euclidean reflection group. More exactly, it is a translation into linear algebra of the geometric configuration formed by the reflecting hyperplanes associated with a reflection group. This reformulation is extremely important. The use of linear algebra enables us to analyze finite reflection groups with great efficiency. All of Chapters 2, 3, 4 and 6 will be devoted to the justification of this remark.

2-1 Root systems

A root system is a set of vectors satisfying certain axioms. To motivate these axioms, we begin by considering the reflecting hyperplanes of a finite Euclidean reflection group. As already suggested in §1-6, the geometric configuration formed by these hyperplanes and, in particular, by the system of associated Weyl chambers, gives a significant amount of information about the structure of the reflection group. The reflection group permutes these hyperplanes, and it is this action that shapes the configuration of the hyperplanes and also provides the link between the resulting geometric pattern and the structure of the reflection group.

We want to understand the symmetrical, and highly restricted, patterns formed by the hyperplanes (and how these patterns are related to the structure of the reflection group). In dimension two, as was illustrated in §1-6, the geometric patterns are easy to analyze: we can simply draw a picture. In higher dimensions, the procedure is not so simple: we cannot analyze the pattern by pictures. The solution is to turn to linear algebra. We replace the reflecting hyperplanes by an equivalent set of vectors, and understand the geometric pattern of the hyperplanes through the linear algebra of the vectors. The other important feature we are concerned about, the action of the reflection group on the geometry, will also turn out to be captured by using linear algebra.

Let $W \subset O(\mathbb{E})$ be a finite reflection group in Euclidean space $\mathbb{E}$. Replace each reflecting hyperplane of W by its two orthogonal vectors of unit length. Let $\Delta \subset \mathbb{E}$ be the resulting set of vectors. Letting s_α be the reflection associated to α as in §1-1, Δ can be described as

$$\Delta = \{\alpha \mid s_\alpha \text{ is a reflection in } W \text{ and } ||\alpha|| = 1\}.$$

We have obtained a set that determines W and its reflecting hyperplanes. For W can be described as the group generated by $\{s_\alpha \mid \alpha \in \Delta\}$, while the reflecting hyperplanes of W consist of $\{H_\alpha \mid \alpha \in \Delta\}$, where

$$H_\alpha = \{x \in \mathbb{E} \mid (x, \alpha) = 0\}.$$

The vectors of Δ satisfy certain properties, firstly:

(B-1) If $\alpha \in \Delta$, then $\lambda\alpha \in \Delta$ if and only if $\lambda = \pm 1$.

Secondly, the set Δ is permuted under the action of W. This permutation property can be expressed by:

(B-2) If $\alpha, \beta \in \Delta$, then $s_\alpha \cdot \beta \in \Delta$.

We have already observed, in §1-6, that the reflecting hyperplanes are permuted by the action of W. Property (B-2) is a reformulation of this property in terms of the orthogonal unit vectors. To give a direct proof, we know that $s_\alpha s_\beta s_\alpha \in W$. And by property (A-4) of §1-1, $s_\alpha s_\beta s_\alpha = s_{s_\alpha \cdot \beta}$. Since s_α is an orthogonal transformation and $\|\beta\| = 1$, we must therefore have $\|s_\alpha \cdot \beta\| = 1$. So $s_\alpha \cdot \beta \in \Delta$.

Definition: A *root system* is a finite set of nonzero vectors $\Delta \subset \mathbb{E}$ satisfying (B-1) and (B-2). Each element of Δ is called a *root*.

Observe that, despite the above example, this definition does not require the vectors to be of unit length. If this extra property is also satisfied, then we shall speak of the root system as being *unitary*. The above discussion demonstrates that every Euclidean reflection group possesses an unitary root system.

Remark 1: The traditional definition of a root system (arising out of Lie theory) incorporates additional properties as well, which are called *crystallographic* and *essential*, and will be treated in §2-3 and in §2-4. Root systems with these extra properties arise in a number of contexts, notably in the study of Lie algebras and algebraic groups. In particular, there is a standard one-to-one correspondence between essential crystallographic root systems and finite dimensional semisimple Lie algebras over $\mathbb{C}$, described in Appendix D. Such root systems will be discussed and studied in Chapters 9–13. It should be noted that, in the literature dealing with Lie algebras, Lie groups and algebraic groups, "root system" typically refers to what we shall call an essential crystallographic root system. In other words, the crystallographic and essential conditions are simply regarded as part of the definition of a root system.

A root system, as defined using properties (B-1) and (B-2), is a linear algebra version of a finite Euclidean reflection group. Given a root system $\Delta \subset \mathbb{E}$, we can convert it into a finite Euclidean reflection group. Namely, let

$$W(\Delta) = \text{the reflection group generated by } \{s_\alpha \mid \alpha \in \Delta\}.$$

The finiteness of $W(\Delta)$ follows from the fact that we have an inclusion

$$W(\Delta) \subset \mathrm{Perm}(\Delta),$$

where $\mathrm{Perm}(\Delta)$ is the (finite!) permutation group of the set Δ. Property (B-2) gives the map from $W(\Delta)$ to $\mathrm{Perm}(\Delta)$. Injectivity of this map follows from the fact that

$$\mathbb{E} = \mathbb{E}_\Delta \oplus \mathbb{E}^\Delta,$$

where $\mathbb{E}_\Delta$ is the subspace spanned by Δ, while $\mathbb{E}^\Delta = \bigcap_{\alpha \in \Delta} H_\alpha$ is the subspace on which $W(\Delta)$ acts trivially. So if φ fixes Δ, then $\varphi = 1$.

We now have a map

$$\{\text{root systems}\} \to \{\text{finite Euclidean reflection groups}\}$$
$$\Delta \to W(\Delta).$$

This map is many to one. As the subsequent discussion will demonstrate, each Euclidean reflection group arises from many different root systems. The procedure of constructing a root system by choosing the orthogonal unit vectors of the reflecting planes shows that the map is surjective.

Length and Root Systems Given a root system Δ, we can vary the lengths of vectors in Δ without affecting $W(\Delta)$. This is based on the observation from §1-1 that $s_\alpha = s_{k\alpha}$ for any $0 \neq k \in \mathbb{R}$. It should be noted, however, that the lengths of root vectors cannot be altered arbitrarily to obtain another root system. The ability to alter root lengths is limited by the action of the associated reflection group. A root system Δ is invariant under the action of $W = W(\Delta)$ and, if two elements of Δ lie in the same W orbit, then they must have the same length; for the elements of W are orthogonal transformations and, hence, preserve length. But, provided we respect the orbit structure of Δ, we can choose the lengths of vectors at will and obtain other root systems with the same reflection group.

Angles and Root Systems As we proceed, it will become clearer that it is the angles between the vectors, and not their length, that contain the essential information about the reflection group. Unlike length, altering the direction of root vectors does change the associated reflection group. This fact will be formalized in Chapter 6, when we deal with Coxeter groups and Coxeter systems.

Remark 2: The above discussion suggests that it would be useful to introduce an appropriate version of "isomorphism" for root systems so that the many different choices of root systems for a given reflection group would be isomorphic. However, an appropriate version (at least if it is to involve a linear isomorphism of the ambient spaces) does not exist at this level. We shall defer discussing isomorphisms of root systems until Chapter 10 when we do so for the particular case of crystallographic root systems. In that case, an effective and useful version can be defined.

The rank of a root system $\Delta \subset \mathbb{E}$ is the dimension of the subspace $\mathbb{E}_\Delta \subset \mathbb{E}$ spanned by the root vectors. In view of the above discussion, we can also talk about the *rank of a reflection group*; for if $W(\Delta) = W(\Delta')$, then Δ and Δ' span the same subspace of $\mathbb{E}$ (roots from one of the root systems are multiples of roots in the other), and hence have the same rank. It therefore makes sense to define the rank of a reflection group as the rank of any associated root system.

A root system $\Delta \subset \mathbb{E}$ will be said to be *reducible* if there is an orthogonal decomposition $\Delta = \Delta_1 \coprod \Delta_2$ of Δ, where $\Delta_1 \neq \varnothing$ and $\Delta_2 \neq \varnothing$ are root systems. (Actually, the property that Δ_1 and Δ_2 are root systems is redundant, i.e., it is forced by the other properties.) Otherwise, a root system will be said to be

irreducible. Reducibility for a root system Δ corresponds to reducibility for its associated reflection group $W(\Delta)$, namely:

Lemma *A root system Δ is reducible if and only if its associated reflection group $W(\Delta)$ is reducible.*

Proof It is clear that the decomposition $\Delta = \Delta_1 \coprod \Delta_2$ induces a reflection group decomposition

$$W(\Delta) = W(\Delta_1) \times W(\Delta_2).$$

Conversely, assume that we have a reflection group decomposition $W(\Delta) = W_1 \times W_2$. We can choose disjoint root systems $\Delta_1 \subset \Delta$ and $\Delta_2 \subset \Delta$, where $W_1 = W(\Delta_1)$ and $W_2 = W(\Delta_2)$. To do this, we let

$$\Delta_1 = \{\alpha \in \Delta \mid s_\alpha \in W_1\}$$
$$\Delta_2 = \{\alpha \in \Delta \mid s_\alpha \in W_2\}.$$

Regarding the properties of root systems, property (B-1) is obvious. To verify property (B-2), use property (A-4) from §1-1. For example, by that property, $s_\alpha, s_\beta \in W_1$ implies $s_{s_\alpha \cdot \beta} = s_\alpha s_\beta s_\alpha \in W_1$. Hence, $\alpha, \beta \in \Delta_1$ implies $s_\alpha \cdot \beta \in \Delta_1$.

We can finish the proof of the lemma by showing that Δ_1 and Δ_2 give an orthogonal decomposition $\Delta = \Delta_1 \coprod \Delta_2$.

(i) Δ_1 and Δ_2 are orthogonal.

This follows from the fact that elements of W_1 commute with elements of W_2; for given $\alpha \in \Delta_1$ and $\beta \in \Delta_2$, then $s_\alpha s_\beta s_\alpha = s_\beta$ forces $s_\alpha \cdot \beta = \mp\beta$ (see property (A-4) of §1-1). Now, α and β are not multiples of each other, so $(\alpha, \beta) \neq 0$ forces

$$s_\alpha \cdot \beta = \beta - \frac{2(\alpha,\beta)}{(\alpha,\alpha)}\alpha \neq \mp\beta.$$

We conclude that $(\alpha, \beta) = 0$.

We are left with showing that

(ii) the inclusion $\Delta_1 \coprod \Delta_2 \subset \Delta$ is an equality.

Given $\alpha \in \Delta$, we want to show either $\alpha \in \Delta_1$ or $\alpha \in \Delta_2$. Equivalently, we want to show that $s_\alpha \in W_1$ or $s_\alpha \in W_2$, i.e., when we write $s_\alpha = (s_1, s_2)$ in $W_1 \times W_2$ we must have either $s_1 = 1$ or $s_2 = 1$. As already observed, we have inclusions $W_1 \subset \mathrm{Perm}(\Delta_1)$ and $W_2 \subset \mathrm{Perm}(\Delta_2)$; so it suffices to show that s_α fixes either Δ_1 or Δ_2. But let H_α be the reflection hyperplane of s_α. Since Δ_1 and Δ_2 span orthogonal subspaces, and since H_α is a hyperplane, we must have either $\Delta_1 \subset H_\alpha$ or $\Delta_2 \subset H_\alpha$. ■

In Chapters 4, 6 and 7 we shall study finite reflection groups through the linear algebra of their associated root systems. From now on, we shall use the notation $W(\Delta)$ to denote a finite reflection group with the understanding that Δ is an associated root system. In all that follows, it will make little difference which associated root system of a reflection group we choose. However, unitary root systems,

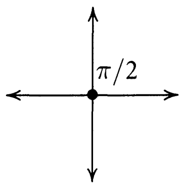
as constructed above, provide canonical choices of a root system associated with each reflection group. By and large, it is unitary root systems that we shall use in our study of finite reflection groups.

2-2 Examples of root systems

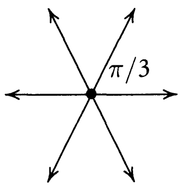
We now give some examples of root systems. We shall be indexing root systems by their rank.

(a) Examples in $\mathbb{R}^2$

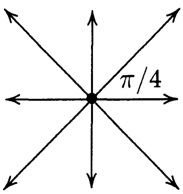
We have already seen that the dihedral groups are the only reflection groups in the plane. So any root system Δ in the plane must have some D_n as its associated Weyl group $W(\Delta)$. Below are three examples. In the last example we have chosen the root vectors so as to have two different lengths. As we mentioned in §2-1, our ability to choose the length of the root vectors is only limited by the action of the associated reflection group $W = W(\Delta)$. If two elements of Δ lie in the same W orbit, then they must have the same length. In the last example, the root vectors fall into two distinct orbits: one orbit consists of the slanted vectors, the other orbit consists of the horizontal and vertical vectors. So the lengths of these two sets of vectors are independent of each other. On the other hand, in the second example, all six vectors lie in one orbit and must, therefore, have the same length.



$W(\Delta) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$



$W(\Delta) = D_3 = \Sigma_3$



$W(\Delta) = D_4$

(b) Root System A_ℓ

Let $\{\epsilon_1, \epsilon_2, \dots, \epsilon_{\ell+1}\}$ be an orthonormal basis of $\mathbb{E} = \mathbb{R}^{\ell+1}$. Choose $\Delta \subset \mathbb{E}$ by letting

$$\Delta = \{\epsilon_i - \epsilon_j \mid i \neq j\}.$$

Then Δ is a root system. The fact that, given $\alpha \in \Delta$, $\lambda\alpha \in \Delta$ if and only if $\lambda = \pm 1$ follows from inspection. Regarding the fact that $s_\alpha \cdot \beta \in \Delta$ for all $\alpha, \beta \in \Delta$, we need only observe that

$$s_{\epsilon_i - \epsilon_j} = \text{the permutation of } \{\epsilon_1, \epsilon_2, \dots, \epsilon_{\ell+1}\} \text{ which interchanges } \epsilon_i \text{ and } \epsilon_j.$$

To verify this, check the effect of $s_{\epsilon_i - \epsilon_j} \cdot x = x - (\epsilon_i - \epsilon_j, x)(\epsilon_i - \epsilon_j)$ on the basis elements $\{\epsilon_1, \epsilon_2, \dots, \epsilon_{\ell+1}\}$. We now have

$$W(\Delta) = \Sigma_{\ell+1}.$$

The fact that $W(\Delta) \subset \Sigma_{\ell+1}$ follows from the description of $s_{\epsilon_i - \epsilon_j}$ as the permutation (i, j). The fact that $W(\Delta) = \Sigma_{\ell+1}$ follows from the fact that the permutations $\{(i, j)\}$ generate $\Sigma_{\ell+1}$.

Moreover, $W(\Delta) = \Sigma_{\ell+1}$ permutes the basis $\{\epsilon_1, \epsilon_2, \dots, \epsilon_{\ell+1}\}$. So the action of $W(\Delta) = \Sigma_{\ell+1}$ is that of permuting the coordinates of $\mathbb{R}^{\ell+1}$, and the reflection group structure on $\Sigma_{\ell+1}$ is that introduced in §1-1.

We note that this root system is labelled A_ℓ rather than $A_{\ell+1}$, even though it is given as a subset of subspace $\mathbb{R}^{\ell+1}$. This notation follows from the fact that the root system actually lies in a subspace of $\mathbb{R}^{\ell+1}$ of dimension ℓ, and hence has rank ℓ. This fact will be further discussed in §2-4.

(c) Root System B_ℓ

Let $\{\epsilon_1, \epsilon_2, \dots, \epsilon_\ell\}$ be an orthonormal basis of $\mathbb{R}^\ell$ and choose $\Delta \subset \mathbb{R}^\ell$ where

$$\Delta = \{\pm\epsilon_i \pm \epsilon_j \mid i \neq j\} \coprod \{\pm\epsilon_i\}.$$

The reflections corresponding to elements of Δ can be described by their effect on $\{\epsilon_1, \epsilon_2, \dots, \epsilon_\ell\}$. We have

$$s_{\epsilon_i - \epsilon_j} = \text{the permutation interchanging } \epsilon_i \text{ and } \epsilon_j$$

$$s_{\epsilon_i} = \text{sign change on } \epsilon_i$$

$$s_{\epsilon_i + \epsilon_j} = \text{permutation which interchanges } \epsilon_i \text{and } \epsilon_j \text{ and changes their sign.}$$

We can deduce from the above descriptions that $W(\Delta) = (\mathbb{Z}/2\mathbb{Z})^\ell \rtimes \Sigma_\ell$ where

$$\Sigma_\ell = \text{the permutation group on } \{\epsilon_1, \dots, \epsilon_\ell\}$$

$$(\mathbb{Z}/2\mathbb{Z})^\ell = \text{sign changes on } \{\epsilon_1, \dots, \epsilon_\ell\}.$$

So $W(\Delta)$ is the reflection group introduced in §1-3 and identified in §1-5 with the symmetry group of the ℓ-cube. In particular, the action of Σ_ℓ on $(\mathbb{Z}/2\mathbb{Z})^\ell$ giving the semidirect product structure for $W(\Delta)$ is that of permuting factors.

***(d) Root System** C_ℓ*

The root system C_ℓ is a minor variant of the B_ℓ root system. Let $\{\epsilon_1, \epsilon_2, \dots, \epsilon_\ell\}$ be an orthonormal basis of $\mathbb{R}^\ell$ and choose $\Delta \subset \mathbb{R}^\ell$ where

$$\Delta = \{\pm\epsilon_i \pm \epsilon_j \mid i \neq j\} \coprod \{\pm 2\epsilon_i\}.$$

From the viewpoint of reflection groups, this root system does not give anything new. The reflection group produced by it is clearly the same as that associated with B_ℓ. The reason for interest in this root system will only become apparent when crystallographic root systems are discussed and classified in Chapters 9 and 10. Both B_ℓ and C_ℓ are part of the classification result obtained there.

***(e) Root System** D_ℓ*

We can locate within the root system B_ℓ a smaller root system. Let $\{\epsilon_1, \dots, \epsilon_\ell\}$ be a orthonormal basis of $\mathbb{R}^\ell$, and let

$$\Delta = \{\pm\epsilon_i \pm \epsilon_j \mid i \neq j\}.$$

This is a root system, and

$$W(\Delta) = (\mathbb{Z}/2\mathbb{Z})^{\ell-1} \rtimes \Sigma_\ell,$$

where

$$\begin{aligned} \Sigma_\ell &= \text{the permutation group on } \{\epsilon_1, \dots, \epsilon_\ell\} \\ (\mathbb{Z}/2\mathbb{Z})^{\ell-1} &= \text{sign changes on an even number of } \{\epsilon_1, \dots, \epsilon_\ell\}. \end{aligned}$$

A more complete list of root systems is given in §8-6.

2-3 Crystallographic root systems

Although we shall be primarily be using unitary root systems in the next few chapters, it is worthwhile remarking that some of the nonunitary root systems are extremely important. Noteworthy among such root systems are those that possess the special property of being *crystallographic*. This means that, besides properties (B-1) and (B-2), the root system Δ also satisfies

(B-3) $\dfrac{2(\alpha, \beta)}{(\alpha, \alpha)} \in \mathbb{Z}$ for any $\alpha, \beta \in \Delta$.

As already mentioned in §2-1, crystallographic root systems are important in a variety of mathematical contexts. A fact not unrelated to this one is that, when we

start looking for examples of root systems, it is crystallographic root systems that occur most naturally. If we consider the examples of root systems in §2-2, most of them are crystallographic. It is crystallographic root systems that predominate in the concrete occurrences of Euclidean reflection groups. On the other hand, we have need of more than just crystallographic root systems. For example, none of the associated root systems of the automorphism group of the dodecahedron (see §1-5) is crystallographic. Again, the associated root system of a dihedral group D_n (see §1-3 and §1-4) can be chosen to be crystallographic only when $n = 2, 3, 4, 6$.

In terms of the associated reflection group, we might mention that the significance of the crystallographic condition is to give $W(\Delta)$ as a subgroup of $\mathrm{GL}_\ell(\mathbb{Z})$, not just as a subgroup of $\mathrm{GL}_\ell(\mathbb{R})$. (Recall the formula $s_\alpha \cdot x = x - \frac{2(\alpha,\beta)}{(\alpha,\alpha)}\alpha$ from §1-1.) The reflection groups having a crystallographic root system are called *Weyl groups*. Weyl groups and crystallographic root systems will be studied in Chapters 9–13.

2-4 Essential root systems and stable isomorphisms

There is another property of root systems $\Delta \subset \mathbb{E}$ that is also part of the traditional definition of a root system. This is the property

(B-4) Δ spans $\mathbb{E}$.

Root systems satisfying (B-4) will be called *essential*, and the associated reflection group will also be called essential. This property will play a significant role in future discussions.

Examples: Except for A_ℓ, the examples of root systems from §2-2 are essential. Consider the reflection group $W(A_\ell) = \Sigma_{\ell+1}$. As discussed in §2-2, it is a reflection group when acting on $\mathbb{R}^{\ell+1}$ by permuting factors. However, the root system $\Delta = A_\ell = \{\epsilon_i - \epsilon_j \mid i \neq j\}$ for this reflection group actually lies in, and spans, the subspace $\mathbb{E} \subset \mathbb{R}^{\ell+1}$ given by

$$\mathbb{E} = \left\{ \sum_{i=1}^{\ell+1} c_i \epsilon \;\middle|\; c_i \in \mathbb{R}, \sum_{i=1}^{\ell+1} c_i = 0 \right\}.$$

$\Sigma_{\ell+1}$ is an essential reflection group when acting on $\mathbb{E} = \mathbb{R}^\ell$, but not when acting on the larger space $\mathbb{R}^{\ell+1}$.

This example illustrates how we can always arrange the property of Δ being essential. If Δ does not span $\mathbb{E}$, then replace $\mathbb{E}$ by the subspace

$$\mathbb{E}_\Delta \subset \mathbb{E},$$

which is spanned by Δ, and consider the induced action of $W(\Delta)$ on $\mathbb{E}_\Delta$. Since $W(\Delta)$ permutes the elements of Δ, the subspace $\mathbb{E}_\Delta \subset \mathbb{E}$ is stable under the action of $W(\Delta)$ on $\mathbb{E}$. Moreover, no significant information is lost in restricting to $\mathbb{E}_\Delta \subset \mathbb{E}$. For the orthogonal complement to $\mathbb{E}_\Delta$ is $\bigcap_{\alpha\in\Delta} H_\alpha$ and $W(\Delta)$ acts trivially on $\bigcap_{\alpha\in\Delta} H_\alpha$.

The observation that we can restrict attention to $\mathbb{E}_\Delta \subset \mathbb{E}$ can be more formally stated by the concept of *stable isomorphism*. As already observed, given a reflection group $W \subset O(\mathbb{E})$, then the subspace $\mathbb{E}_\Delta \subset \mathbb{E}$ is the same for every root system $\Delta \subset \mathbb{E}$ of W. (Roots from one of the root systems are multiples of roots in the other.) So we can talk about the subspace

$$\mathbb{E}_W \subset \mathbb{E}$$

of a reflection group $W \subset O(\mathbb{E})$. By the remarks in the previous paragraph, there is an orthogonal decomposition

$$\mathbb{E} = \mathbb{E}_W \oplus \mathbb{E}^W,$$

where

$$\mathbb{E}^W = \{\alpha \in \mathbb{E} \mid \varphi \cdot \alpha = \alpha \text{ for all } \varphi \in W\}$$

consists of the fixed points of W. Furthermore, the reflection group $W \subset O(\mathbb{E})$ actually lies in $O(\mathbb{E}_W)$, i.e., we have inclusions

$$W \subset O(\mathbb{E}_W) \subset O(\mathbb{E}).$$

The next definition generalizes the definition of isomorphic reflection groups given in §1-1.

Definition: Two reflection groups $W \subset O(\mathbb{E})$ and $W' \subset O(\mathbb{E}')$ will be said to be *stably isomorphic* if there exists a linear isomorphism $f\colon \mathbb{E}_W \longrightarrow \mathbb{E}_{W'}$ preserving inner products and conjugating W to W'. In other words,

$$\big(f(\alpha), f(\beta)\big) = (\alpha, \beta) \quad \text{for all } \alpha, \beta \in \mathbb{E}_W$$
$$fWf^{-1} = W'.$$

Every stable isomorphism class is represented uniquely by an essential reflection group. As we have already indicated, essential reflection groups will play an important role in Chapters 6 and 7. There we shall be studying the correlation between the geometry of reflection groups and the algebraic data given by the "Coxeter presentation" of such groups. If we deal with stable isomorphism classes of reflection groups, then this correlation is exact, i.e., the Coxeter presentation gives complete information about the reflection group up to stable isomorphism.

The discussion of the reflection group $W(A_\ell) = \Sigma_{\ell+1}$ provides an example of a stable isomorphism. The two different descriptions given there of $\Sigma_{\ell+1}$ as a reflection group (for $\mathbb{R}^\ell$ and $\mathbb{R}^{\ell+1}$, respectively) are stably isomorphic.

Remark: In Appendix B, stable isomorphisms are further discussed in the context of representation theory. The building blocks of representation theory are irreducible representations. Reflection groups $W \subset O(\mathbb{E})$ are, of course, examples of representations. However, an irreducible reflection group (which was defined

in §1-1) is not quite the same thing as an irreducible representation. The relationship is examined in Appendix B. It is observed that when $W \subset O(\mathbb{E})$ is regarded as a representation $\rho\colon W \to O(\mathbb{E})$, then it can be decomposed into irreducible representations

$$\rho = \rho_1 \oplus \cdots \oplus \rho_k,$$

where each ρ_i is either a reflection representation or the trivial representation. It is easy to deduce from this fact that a reflection group is an irreducible representation if and only if it is both essential and irreducible as a reflection group.

In all that follows (see, in particular, Chapters 6–8) we will be dealing with irreducible reflection groups classified up to stable isomorphism. So this corresponds exactly to determining the finite Euclidean reflection groups that are irreducible representations.

3 Fundamental systems

In this chapter we introduce fundamental systems for root systems. Just as a root system is a translation into linear algebra of the reflecting hyperplanes of a finite reflection group, so a fundamental system is a linear algebra version of a Weyl chamber of the group. The discussion of fundamental systems in this chapter largely amounts to the construction of a one-to-one correspondence between chambers and fundamental systems. We shall also introduce, in the final section of this chapter, the important concept of height.

Fundamental systems will play an important role in our analysis of finite Euclidean reflection groups. As we shall see in Chapter 4 a fundamental system gives rise to an optimal set of generators for a reflection group. In particular, in Chapter 6 we shall use such generators to obtain the "Coxeter presentation" of a reflection group.

3-1 Fundamental systems

In this chapter we shall demonstrate that every root system $\Delta \subset \mathbb{E}$ contains a very special type of generating set. In this section, we introduce the concept of a fundamental system, whereas in subsequent sections we address the questions of existence and uniqueness of such systems.

Definition: Given a root system $\Delta \subset \mathbb{E}$, then $\Sigma \subset \Delta$ is a *fundamental system* of Δ if

(i) Σ is linearly independent
(ii) every element of Δ is a linear combination of elements of Σ, where the coefficients are all nonnegative or all nonpositive.

The elements of Σ are called *fundamental roots*. Other terms commonly used for Σ are *base* or *simple system*. In the latter case, the elements of Σ are called *simple roots*.

The elements of Δ that can be expanded in terms of Σ with coefficients ≥ 0 will be called *positive roots*, while those that can be expanded in terms of Σ with coefficients ≤ 0 will be called *negative roots*. In particular, the elements of Σ are positive. We shall use the notation

$$\alpha > 0 \quad \text{and} \quad \alpha < 0$$

to indicate whether a given $\alpha \in \Delta$ is positive or negative with respect to Σ. If we let Δ^+ and Δ^- denote the positive and negative roots, then we have the decomposition

$$\Delta = \Delta^+ \coprod \Delta^- .$$

There is a very close relation between a fundamental system Σ and this associated decomposition of Δ. Besides Σ determining $\Delta = \Delta^+ \coprod \Delta^-$, the decomposition $\Delta = \Delta^+ \coprod \Delta^-$ also determines Σ. This relation will be discussed in §3-4.

Observe that it is not clear from the definition whether fundamental systems actually exist for any given root system. In fact they do. But existence is a nontrivial matter. We shall explain how to construct a fundamental system in §3-3. Fundamental systems are far from unique. Notably, the elements of $W(\Delta)$, as they permute the elements of Δ, must send a fundamental system to another fundamental system. So any fundamental system gives rise to more of the same. The question of how many fundamental systems a root system can possess will be discussed in §3-5. By the end of that discussion, we shall have established a one-to-one correspondence

$$\{\text{chambers}\} \longleftrightarrow \{\text{fundamental systems}\}.$$

The passage from fundamental systems to chambers is particularly easy to state. If $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$ is a fundamental system, then

$$\mathcal{C} = \{t \in \mathbb{E} \mid (t, \alpha_i) > 0 \text{ for } i = 1, \ldots, \ell\}$$

is the corresponding chamber (see §3-5). This will be called the *fundamental chamber* with respect to Σ.

3-2 Examples of fundamental systems

We return to the root systems A_ℓ, B_ℓ, C_ℓ, D_ℓ considered in §2-2, and demonstrate that these root systems possess fundamental systems. All of the notation from §2-2 will be assumed in the following discussion.

(a) Root System A_ℓ

We have $\Delta = \{\epsilon_i - \epsilon_j \mid i \neq j\}$. The canonical choice of a fundamental system for Δ is

$$\Sigma = \{\epsilon_1 - \epsilon_2, \epsilon_2 - \epsilon_3, \ldots, \epsilon_\ell - \epsilon_{\ell+1}\}.$$

Then

$$\Delta^+ = \{\epsilon_i - \epsilon_j \mid i < j\} \quad \text{and} \quad \Delta^- = \{\epsilon_i - \epsilon_j \mid i > j\}.$$

For, given $i < j$, then

$$\begin{aligned} \epsilon_i - \epsilon_j &= (\epsilon_i - \epsilon_{i+1}) + (\epsilon_{i+1} - \epsilon_{i+2}) + \cdots + (\epsilon_{j-1} - \epsilon_j) \\ \epsilon_j - \epsilon_i &= -(\epsilon_i - \epsilon_{i+1}) - (\epsilon_{i+1} - \epsilon_{i+2}) - \cdots - (\epsilon_{j-1} - \epsilon_j). \end{aligned}$$

There are many other possible choices of a fundamental system. We have already remarked in §3-1 that, if we apply any element of $W(\Delta) = \Sigma_{n+1}$ to the above, then we obtain another fundamental system. In other words, if we take any permutation $\{i_1, \ldots, i_{\ell+1}\}$ of $\{1, \ldots, \ell+1\}$, then $\{\epsilon_{i_1} - \epsilon_{i_2}, \epsilon_{i_2} - \epsilon_{i_3}, \ldots, \epsilon_{i_\ell} - \epsilon_{i_{\ell+1}}\}$ is also a fundamental system for Δ. We shall show in §4-6 that these are all the possibilities for fundamental systems in the A_ℓ case.

(b) Root System B_ℓ

This time $\Delta = \{\pm\epsilon_i \pm \epsilon_j \mid i \neq j\} \coprod \{\pm\epsilon_i\}$, and the canonical choice of a fundamental system is

$$\Sigma = \{\epsilon_1 - \epsilon_2, \epsilon_2 - \epsilon_3, \ldots, \epsilon_{\ell-1} - \epsilon_\ell, \epsilon_\ell\}.$$

For this choice,

$$\Delta^+ = \{\epsilon_i - \epsilon_j \mid i < j\} \coprod \{\epsilon_i + \epsilon_j \mid i \neq j\} \coprod \{\epsilon_i\}$$
$$\Delta^- = \{\epsilon_i - \epsilon_j \mid i > j\} \coprod \{-\epsilon_i - \epsilon_j \mid i \neq j\} \coprod \{-\epsilon_i\}.$$

If we apply elements of $W(\Delta) = (\mathbb{Z}/2\mathbb{Z})^\ell \rtimes \Sigma_\ell$ to the above system, then we obtain other fundamental systems. So we can permute $\{\epsilon_1, \ldots, \epsilon_\ell\}$ in any fashion, as well as change their signs.

(c) Root System C_ℓ

A fundamental system for $\Delta = \{\pm\epsilon_i \pm \epsilon_j \mid i \neq j\} \coprod \{\pm 2\epsilon_i\}$ is given by

$$\Sigma = \{\epsilon_1 - \epsilon_2, \epsilon_2 - \epsilon_3, \ldots, \epsilon_{\ell-1} - \epsilon_\ell, 2\epsilon_\ell\}.$$

It gives the following positive and negative roots:

$$\Delta^+ = \{\epsilon_i - \epsilon_j \mid i < j\} \coprod \{\epsilon_i + \epsilon_j \mid i \neq j\} \coprod \{\epsilon_i\}$$
$$\Delta^- = \{\epsilon_i - \epsilon_j \mid i > j\} \coprod \{-\epsilon_i - \epsilon_j \mid i \neq j\} \coprod \{-\epsilon_i\}.$$

(d) Root System D_ℓ

We have $\Delta = \{\pm\epsilon_i \pm \epsilon_j \mid 1 \leq i, j \leq \ell, i \neq j\}$. This time we can choose

$$\Sigma = \{\epsilon_1 - \epsilon_2, \ldots, \epsilon_{\ell-1} - \epsilon_\ell, \epsilon_{\ell-1} + \epsilon_\ell\}$$

as a fundamental system. And then

$$\Delta^+ = \{\epsilon_i - \epsilon_j \mid i < j\} \coprod \{\epsilon_i + \epsilon_j \mid i \neq j\}$$
$$\Delta^- = \{\epsilon_i - \epsilon_j \mid i > j\} \coprod \{-\epsilon_i - \epsilon_j \mid i \neq j\}.$$

For other choices of fundamental systems, we are allowed to permute $\{1, \ldots, \ell\}$, as well as to change the signs on any even number of $\{\epsilon_1, \ldots, \epsilon_\ell\}$.

3-3 Existence of fundamental systems

We now describe a method for extracting a fundamental system from any given root system $\Delta \subset \mathbb{E}$. Weyl chambers were introduced in §1-6. In this section, we shall show that any Weyl chamber gives rise to a fundamental system. In the next section, we shall show that the choice of the fundamental system (with respect to a given chamber) is unique. There are two steps in constructing the fundamental system.

(I) First, create a candidate for the positive and negative roots by partitioning Δ into two sets $\Delta = \Delta^+ \coprod \Delta^-$.
(II) Next, show that Δ^+ contains a set Σ which is a fundamental system having Δ^+ and Δ^- as its positive and negative roots.

Step I

This step is straightforward. Pick a chamber $\mathcal{C}$ and $t \in \mathcal{C}$. For such a choice to be possible, we need to know that $\mathbb{E} \neq \bigcup_{\alpha\in\Delta} H_\alpha$. This follows from the next lemma.

Lemma A *Let V be a vector space over an infinite field $\mathbb{F}$. Then V is not the union of a finite number of proper subspaces.*

Proof We can assume that $\dim V \geq 2$. We assume that V is the union of a finite number of proper subspaces, and show that this leads to a contradiction. We can reduce to the case where V is a union

$$V = \bigcup_{i=1}^{n} H_i$$

of hyperplanes $\{H_i\}$ and the union is minimal in the sense that, for each i, $V_i \neq V$ where

$$V_i = H_1 \cup \cdots \cup H_{i-1} \cup H_{i+1} \cup \cdots \cup H_n.$$

For each i, one can choose β_i satisfying

$$\beta_i \in H_i \quad \text{and} \quad \beta_i \notin H_j \quad \text{for } j \neq i$$

(just pick $\beta_i \in H_i$ so that $\beta_i \notin V_i$). Since $\mathbb{F}$ is infinite, the set $\{\beta_1 + \lambda\beta_2 \mid \lambda \in \mathbb{F}\}$ is also infinite. Hence, there exists $0 \neq \lambda, \lambda' \in \mathbb{F}$ such that $\beta_1 + \lambda\beta_2$ and $\beta_1 + \lambda'\beta_2$ both belong to the same H_k. Thus

$$(\lambda - \lambda')\beta_2 = (\beta_1 + \lambda\beta_2) - (\beta_1 + \lambda'\beta_2) \in H_k$$

as well. Since $\lambda - \lambda' \neq 0$, it follows that $\beta_2 \in H_k$. So we must have $k = 2$. But then $\beta_1 + \lambda\beta_2 \in H_2$ and $\beta_2 \in H_2$ also forces $\beta_1 \in H_2$, a contradiction. ■

Since $t \notin H_\alpha$ for all $\alpha \in \Delta$, we have $(t, \alpha) \neq 0$ for all $\alpha \in \Delta$. Let

$$\Delta^+ = \{\alpha \in \Delta \mid (t, \alpha) > 0\}$$
$$\Delta^- = \{\alpha \in \Delta \mid (t, \alpha) < 0\}.$$

The partition $\Delta = \Delta^+ \coprod \Delta^-$ only depends on the choice of the chamber $\mathcal{C}$. It is independent of the choice of any particular $t \in \mathcal{C}$. For, as discussed in §1-6, given t and t' in $\mathbb{E} - (\bigcup_{\alpha\in\Delta}^{\ell} H_\alpha)$, then t and t' are in the same chamber if and only if they are on "the same side" of each hyperplane H_α, i.e., (t, α) and (t', α) must have the same sign for each $\alpha \in \Delta$.

Step II

The extraction of a fundamental system Σ from Δ^+ demands more work. The choice of the set Σ is easy to describe. Choose $\Sigma \subset \Delta^+$, where:

(a) every element in Δ^+ is a linear combination of Σ with coefficients ≥ 0
(b) no subset of Σ satisfies (a).

Justifying that Σ is a fundamental system amounts to showing that Σ is linearly independent. First of all, as a preliminary, we have:

Lemma B *Given $\alpha, \beta \in \Sigma$ where $\alpha \neq \beta$, then $(\alpha, \beta) \leq 0$.*

Proof Suppose $(\alpha, \beta) > 0$. We shall show that this is impossible. The reflection s_α satisfies $s_\alpha \cdot \beta = \beta - \lambda\alpha$, where $\lambda = \frac{2(\alpha,\beta)}{(\alpha,\alpha)} > 0$. To see what is wrong with this, we must consider the two separate possibilities for $s_\alpha \cdot \beta$.

(i) $s_\alpha \cdot \beta \in \Delta^+$.

Then $\beta - \lambda\alpha = s_\alpha \cdot \beta = \sum_i \lambda_i \alpha_i$, where $\lambda_i \geq 0$ and $\alpha_i \in \Sigma$. So

$$(*) \qquad \beta = \lambda\alpha + \sum_i \lambda_i \alpha_i.$$

Now $\beta = \alpha_i$ for some i. So we can speak of the coefficient of β in the RHS of $(*)$. If the coefficient of β in the RHS < 1, then β is a positive linear combination of the remaining elements of Σ. If the coefficient of β in the RHS ≥ 1, then 0 is a positive linear combination of elements of Σ. In both cases, there is a contradiction. The first case contradicts property (b) of Σ. The second case contradicts the fact that any positive linear combination of elements of Σ is nonzero when evaluated on the chamber $\mathcal{C}$.

(ii) $-s_\alpha \cdot \beta \in \Delta^+$.

This time we have $-\beta + \lambda\alpha = -s_\alpha \cdot \beta = \sum_i \lambda_i \alpha_i$, and so

$$(**) \qquad \lambda\alpha = \beta + \sum_i \lambda_i \alpha_i.$$

As with $(*)$ this equation produces a contradiction. The two cases we consider are: the coefficient of α in the RHS of $(**) < \lambda$ and the coefficient of α in the RHS of $(**) \geq \lambda$. ∎

We can use Lemma B to prove:

Lemma C *Σ is linearly independent.*

Proof Any relation of linear dependence can be converted into an equation

$$\sum_i a_i \alpha_i = \sum_j b_j \beta_j,$$

where $a_i \geq 0$, $b_j \geq 0$ and $\{\alpha_i\} \coprod \{\beta_j\}$ are distinct elements of Σ. So it suffices to show that, for any such equation, $a_i = 0 = b_j$ for all i, j. Let

$$v = \sum_i a_i \alpha_i = \sum_j b_j \beta_j.$$

Then, by Lemma B, $(v, v) = \sum_{i,j} a_i b_j (\alpha_i, \beta_j) \leq 0$. Since $(v, v) \geq 0$, we must have $(v, v) = 0$. Thus $v = 0$. The equations $\sum_i a_i \alpha_i = 0 = \sum b_j \beta_j$ force $\alpha_i = 0 = \beta_j$. Otherwise, we could write 0 as a positive linear combination of elements of Σ. This contradicts the fact that any such linear combination is nonzero when evaluated on the chamber $\mathcal{C}$. ∎

3-4 Fundamental systems and positive roots

In this section, we prove that two fundamental systems giving rise to the same decomposition $\Delta = \Delta^+ \coprod \Delta^-$ must be the same. In particular, this guarantees that the choice of the fundamental system associated with a given chamber, as explained in §3-3, is unique. In other words, once we have used the chamber $\mathcal{C}$ to make the decomposition $\Delta = \Delta^+ \coprod \Delta^-$, there is only one fundamental system that can give rise to this decomposition. So we have a well-defined map

$$\Psi\colon \{\text{chambers}\} \to \{\text{fundamental systems}\}.$$

This map will be studied further in §3-5. The rest of this section is devoted to the proof of:

Proposition *Let Δ be a root system. Let Σ_1 and Σ_2 be fundamental systems of Δ and let*

$$\Delta = \Delta_1^+ \coprod \Delta_1^- \quad \textit{and} \quad \Delta = \Delta_2^+ \coprod \Delta_2^-$$

be the associated decompositions of Δ into positive and negative roots. Then $\Sigma_1 = \Sigma_2$ if and only if $\Delta_1^+ = \Delta_2^+$.

First of all, it is trivial that $\Sigma_1 = \Sigma_2$ forces $\Delta_1^+ = \Delta_2^+$. So suppose $\Delta_1^+ = \Delta_2^+$. We want $\Sigma_1 = \Sigma_2$. Write

$$\Sigma_1 = \{\alpha_1, \ldots, \alpha_\ell\} \quad \text{and} \quad \Sigma_2 = \{\beta_1, \ldots, \beta_\ell\}.$$

Since $\Delta_1^+ = \Delta_2^+$, we have

$$\alpha_i = \sum_j x_{ij} \beta_j \quad \text{where } x_{ij} \geq 0$$

$$\beta_i = \sum_j y_{ij} \alpha_j \quad \text{where } y_{ij} \geq 0.$$

Observe that the matrices $[x_{ij}]_{\ell\times\ell}$ and $[y_{ij}]_{\ell\times\ell}$ must be inverses of each other. The main step in the proof is to show:

Lemma *$[x_{ij}]_{\ell\times\ell}$ is a monomial matrix (i.e., each row and column has exactly one nonzero entry).*

For, if the lemma holds, then, by reindexing $\{\alpha_1, \dots, \alpha_\ell\}$ and $\{\beta_1, \dots, \beta_\ell\}$, we can assume $[x_{ij}]_{\ell\times\ell}$ is a diagonal matrix. But this forces $[x_{ij}]_{\ell\times\ell}$ to be the identity matrix. For, if $\alpha_i = \alpha_{ij}\beta_i$ where $x_{ij} > 0$, then, by property (B-1) of a root system, we must have $x_{ij} = 1$. So we are left with proving the lemma.

Proof of Lemma The proof will be done in three steps.

(i) If $x_{ij} \neq 0$, then $y_{jk} = 0$ when $k \neq i$.

For $[x_{ij}]_{\ell\times\ell}$ and $[y_{ij}]_{\ell\times\ell}$ being inverse matrices forces $\sum_m x_{im}y_{mk} = 0$ for $k \neq i$. Since all coefficients are nonnegative, and since $x_{ij} \neq 0$, we must have $y_{jk} = 0$.

(ii) If $y_{jk} = 0$ for $k \neq i$, then $y_{ji} \neq 0$.

Otherwise, the matrix $[y_{ij}]_{\ell\times\ell}$ would have a zero row. So it would not be invertible.

(iii) If $y_{ji} \neq 0$, then $x_{ik} = 0$ for $k \neq j$.

The argument for (iii) is a repetition of that used to prove (i). It follows from (i), (ii) and (iii) that each row of $[x_{ij}]_{\ell\times\ell}$ contains at most one nonzero entry. Since $[x_{ij}]_{\ell\times\ell}$ is invertible, it follows that each row contains at least one nonzero entry. The invertibility of $[x_{ij}]_{\ell\times\ell}$ also now forces each column to have exactly one nonzero entry. ∎

3-5 Weyl chambers and fundamental systems

The procedure described in §3-3 for constructing fundamental systems actually sets up a one-to-one correspondence between Weyl chambers and fundamental systems. As observed at the beginning of §3-4, it gives a well-defined map

$$\Psi\colon \{\text{chambers}\} \to \{\text{fundamental systems}\}.$$

The proof that Ψ is bijective will be done in two steps.

(i) The map Ψ is injective.

The construction in §3-3 has two parts: the choice of the positive roots $\Delta^+ \subset \Delta$ and the choice of the fundamental system $\Sigma \subset \Delta^+$. If two fundamental systems have different positive roots, then they are distinct. (This was the trivial part of Proposition 3-4.) So it suffices to show that different chambers give rise to different partitions $\Delta = \Delta^+ \coprod \Delta^-$. Given a chamber $\mathcal{C}$, Δ^+ (respectively Δ^-) is defined to be the elements of Δ that are positive (respectively negative) on $\mathcal{C}$. Given two distinct chambers, there exists a hyperplane H_α ($\alpha \in \Delta$) separating them. So α is positive for one chamber and negative for the other chamber.

(ii) The map Ψ is surjective.

Suppose we have a fundamental system $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$ of Δ. Let

$$\mathcal{C} = \{t \in \mathbb{E} \mid (t, \alpha_i) > 0 \text{ for } i = 1, \ldots, \ell\}.$$

First of all, $\mathcal{C} \neq \varnothing$. For, if $\{\bar{\alpha}_i\}$ is the dual set of $\{\alpha_i\}$ (i.e., $(\alpha_i, \bar{\alpha}_j) = \delta_{ij}$), then $\bar{\alpha}_1 + \cdots + \bar{\alpha}_\ell \in \mathcal{C}$. Secondly, $\mathcal{C}$ is a chamber. If we consider the positive and negative roots with respect to Σ then, given $t \in \mathcal{C}$, we must have

$$(*) \qquad \begin{aligned} (\alpha, t) &> 0 \quad \text{for } \alpha > 0 \\ (\alpha, t) &< 0 \quad \text{for } \alpha < 0. \end{aligned}$$

Thus all the elements of $\mathcal{C}$ lie on the same side of each hyperplane H_α. By our previous discussion of chambers, this means that $\mathcal{C}$ is a chamber. Finally, by the definition of Ψ, we have $\Psi(\mathcal{C}) = \Sigma$.

Thus we have set up a one-to-one correspondence between Weyl chambers and fundamental systems. As we stated in §3-1, the passage from fundamental systems to chambers is particularly easy to state. If $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$ is a fundamental system, then

$$\mathcal{C} = \{t \in \mathbb{E} \mid (t, \alpha_i) > 0 \; i = 1, \ldots, \ell\}$$

is the corresponding chamber. It will be called the *fundamental chamber* with respect to Σ.

The correspondence between chambers and fundamental systems can also be envisaged in a more geometric way. To explain this approach, we have to introduce the walls of a chamber.

Walls of a Chamber

Given a chamber $\mathcal{C}$, let $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$ be the corresponding fundamental system. The *walls of* $\mathcal{C}$ are the hyperplanes $\{H_{\alpha_1}, H_{\alpha_2}, \ldots, H_{\alpha_\ell}\}$. The term wall arises from the fact that pieces of these hyperplanes form the boundary of $\mathcal{C}$. If $\overline{\mathcal{C}}$ is the *closure* of $\mathcal{C}$, then $\overline{\mathcal{C}} - \mathcal{C}$ lies in $H_{\alpha_1} \cup \cdots \cup H_{\alpha_\ell}$; for we can define $\mathcal{C}$ and $\overline{\mathcal{C}}$ in terms of $\{\alpha_1, \ldots, \alpha_\ell\}$ by

$$\mathcal{C} = \{t \in \mathbb{E} \mid (t, \alpha_i) > 0 \; i = 1, \ldots, \ell\}$$
$$\overline{\mathcal{C}} = \{t \in \mathbb{E} \mid (t, \alpha_i) \geq 0 \; i = 1, \ldots, \ell\}.$$

The hyperplanes $\{H_{\alpha_1}, \ldots, H_{\alpha_\ell}\}$ are distinguished among all the reflecting hyperplanes of W in that they have maximal contact with $\overline{\mathcal{C}}$. We can show that they are the only reflecting hyperplanes whose intersection with $\overline{\mathcal{C}}$ is of dimension $\ell - 1$.

We can also easily specify the fundamental system $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$ associated with the chamber $\mathcal{C}$. Namely, Σ consists of the roots orthogonal to the walls of $\mathcal{C}$ and pointing "into" $\mathcal{C}$. We have already observed that $\{\alpha_1, \ldots, \alpha_\ell\}$ are root vectors orthogonal to the walls of $\mathcal{C}$. The fact that they are the orthogonal root vectors pointing into $\mathcal{C}$ follows from the inequalities

$$\begin{aligned} (\alpha_i, \alpha_i) &> 0 \\ (\alpha_i, \alpha_j) &< 0 \quad \text{for } i \neq j. \end{aligned}$$

The above two paragraphs thus provide another way of relating chambers to fundamental systems.

3-6 Height

In this final section of Chapter 3, we introduce the concept of height and demonstrate its usefulness in studying root systems. Let Δ be a root system with associated reflection group $W = W(\Delta)$. Let $\Sigma = \{\alpha_1, \dots, \alpha_\ell\}$ be a fundamental system of Δ.

Definition: Given $\alpha \in \Delta$, write $\alpha = \sum_i \lambda_i \alpha_i$. Then $h(\alpha) = \sum_i \lambda_i$ is the *height* of α (with respect to Σ).

Height gives us an organizational principle for making inductive arguments. We shall use it in this fashion to prove the next theorem. The concept of an *orbit* is discussed in Appendix B.

Theorem *$\Delta = W \cdot \Sigma$, i.e., every W orbit of Δ contains a fundamental root.*

Remark: In §4-6 we shall show that W acts transitively on $\{$fundamental systems$\}$ $= \{$chambers$\}$. The above theorem when combined with this result shows that every root vector is part of some fundamental system, or, equivalently, that every hyperplane is the wall of some chamber.

The rest of this section will be devoted to the proof of the theorem. If we consider the positive and negative roots determined by Σ, then

$$h(\alpha) > 0 \text{ if } \alpha > 0 \quad \text{and} \quad h(\alpha) < 0 \text{ if } \alpha < 0.$$

The following fact enables us to use height in inductive arguments.

Lemma *Given $\alpha > 0$ where $\alpha \notin \Sigma$, then there exists $\alpha_i \in \Sigma$ such that:*

(i) $s_{\alpha_i} \cdot \alpha > 0$
(ii) $h(s_{\alpha_i} \cdot \alpha) < h(\alpha)$.

Proof Since $\alpha \in \Delta^+ - \Sigma$, it follows that, in the expansion $\alpha = \sum_i \lambda_i \alpha_i$, we have $\lambda_i \geq 0$ and at least two $\lambda_i > 0$. We can choose $\alpha_k \in \Sigma$ so that

$$(*) \qquad (\alpha, \alpha_k) > 0.$$

Otherwise, it would be $(\alpha, \alpha) = \sum \lambda_i (\alpha, \alpha_i) \leq 0$. This in turn forces $(\alpha, \alpha) = 0$, and so $\alpha = 0$. We want to show that

$$(**) \qquad s_{\alpha_k} \cdot \alpha = \alpha - \frac{2(\alpha, \alpha_k)}{(\alpha_k, \alpha_k)} \alpha_k$$

satisfies (i) and (ii) of the lemma. Property (ii) follows from $(*)$. Regarding property (i), observe that $(**)$ implies that if we apply s_{α_k} to $\alpha = \sum \lambda_i \alpha_i$ then the

only coefficient affected is that of α_k. So at least one coefficient is positive when we expand $s_{\alpha_k} \cdot \alpha$ in terms of Σ. Since $s_{\alpha_k} \cdot \alpha \in \Delta = \Delta^+ \coprod \Delta^-$, we must have $s_{\alpha_k} \cdot \alpha > 0$. ■

This lemma has some important consequences for the height of root vectors.

Corollary *Given $\alpha \in \Delta^+$, then $h(\alpha) \geq 1$. Moreover, $h(\alpha) = 1$ if and only if $\alpha \in \Sigma$.*

Proof First of all, $h(\alpha) \geq 1$. For $h(\alpha) < 1$ means that $\alpha \notin \Sigma$. So we can apply the lemma to obtain an element from Δ^+ of even smaller height. By repeating this argument, we would produce an infinite sequence of elements in Δ^+.

Secondly, if $\alpha \in \Sigma$, then $h(\alpha) = 1$. Thirdly, if $h(\alpha) = 1$, then $\alpha \in \Sigma$. For $\alpha \notin \Sigma$ implies that we can apply the lemma to obtain $\bar{\alpha} \in \Delta^+$ of height < 1. ■

We now set about proving our theorem. We shall actually prove a stronger result than that stated by the theorem. This stronger version will be needed in §4-1. Choose a fundamental system Σ of Δ. Let

$$W_0 = \text{the subgroup of } W \text{ generated by } \{s_\alpha \mid \alpha \in \Sigma\}.$$

Proposition *Given $\alpha \in \Delta$, then $\alpha = \varphi \cdot \alpha_k$ for some $\varphi \in W_0$ and $\alpha_k \in \Sigma$.*

Proof We can reduce to $\alpha > 0$. For if $\alpha = \varphi \cdot \alpha_k$, then $-\alpha = \varphi \cdot (-\alpha_k) = (\varphi s_{\alpha_k}) \cdot \alpha_k$. We proceed by induction on $h(\alpha)$. If $h(\alpha) = 1$, then $\alpha \in \Sigma$ and we can let $\varphi = 1$. If $h(\alpha) > 1$, then, by the preceding lemma, we can choose $\alpha_i \in \Sigma$ so that

$$s_{\alpha_i} \cdot \alpha > 0 \quad \text{and} \quad h(s_{\alpha_i} \cdot \alpha) < h(\alpha).$$

By induction, $s_{\alpha_i} \cdot \alpha = \varphi \cdot \alpha_k$ for some $\varphi \in W_0$ and $\alpha_k \in \Sigma$. So $\alpha = (s_{\alpha_i}\varphi) \cdot \alpha_k$. ■

4 Length

This chapter is the first in which we begin to explore the relation between the algebraic structure of a reflection group and its underlying geometry. The main purpose of this chapter is to introduce the concept of length in a reflection group and to explain how length is related to the action of the reflection group on its root system and on its Weyl chambers. The main application of length will come in Chapter 6, when we prove that a finite Euclidean reflection group is a Coxeter group. In particular, the relationship between the algebra and the geometry of Euclidean reflection groups will become more apparent in that chapter.

4-1 Fundamental reflections

In order to define the concept of length in a reflection group, we need a canonical set of generators for the group. Let $W \subset O(\mathbb{E})$ be a finite Euclidean reflection group and let $\Delta \subset \mathbb{E}$ be a root system of W.

Definition: The reflections $\{s_\alpha \mid \alpha \in \Sigma\}$ corresponding to a fundamental system Σ of Δ are called a set of *fundamental reflections* for W.

Proposition *Given any fundamental system Σ of Δ, then $W = W(\Delta)$ is generated by the fundamental reflections $\{s_\alpha \mid \alpha \in \Sigma\}$.*

Proof As in §3-6, let $W_0 =$ the subgroup of W generated by $\{s_\alpha \mid \alpha \in \Sigma\}$. To show $W_0 = W$ it suffices to show $s_\alpha \in W_0$ for all $\alpha \in \Delta$. Proposition 3-6 states that:

$$\text{given } \alpha \in \Delta, \text{ then } \alpha = \varphi \cdot \alpha_k \text{ for some } \varphi \in W_0 \text{ and } \alpha_k \in \Sigma.$$

By property (A-4) of §1-1, the identity $\alpha = \varphi \cdot \alpha_k$ forces $s_\alpha = \varphi s_{\alpha_k} \varphi^{-1}$. This identity, in turn, implies that $s_\alpha \in W_0$. ∎

Examples: We shall illustrate the above proposition for the Euclidean reflection groups associated with the root systems A_ℓ and B_ℓ. These root systems and their fundamental systems were discussed in §2-4 and §3-2. We refer to those sections for the notation used below.

(a) Root System A_ℓ

We have $\Delta = \{\epsilon_i - \epsilon_j \mid i \neq j\}$ with

$$\Sigma = \{\epsilon_1 - \epsilon_2, \epsilon_2 - \epsilon_3, \ldots, \epsilon_\ell - \epsilon_{\ell+1}\}$$

as a fundamental system of Δ. Also,

$$W(\Delta) = \Sigma_{\ell+1}, \text{ the permutations of } \{\epsilon_1, \epsilon_2, \ldots, \epsilon_{\ell+1}\},$$

with the reflection $s_{\epsilon_i - \epsilon_j}$ being the involution interchanging ϵ_i and ϵ_j. If we regard $W(\Delta)$ as the permutations of $\{1, \ldots, \ell + 1\}$, then $s_{\epsilon_i - \epsilon_j}$ is the transposition

(i, j) and so the fundamental reflections determined by Σ are the permutations $\{(1,2),(2,3),(3,4),\ldots,(\ell,\ell+1)\}$. It is well known that these permutations generate all the permutations in $\Sigma_{\ell+1}$.

(b) Root System B_ℓ

This time $\Delta = \{\pm\epsilon_i \pm \epsilon_j \mid i \neq j\} \coprod \{\pm\epsilon_i\}$ with

$$\Sigma = \{\epsilon_1 - \epsilon_2, \epsilon_2 - \epsilon_3, \ldots, \epsilon_{\ell-1} - \epsilon_\ell, \epsilon_\ell\}$$

being a fundamental system. Also,

$$W(\Delta) = (\mathbb{Z}/2\mathbb{Z})^\ell \rtimes \Sigma_\ell,$$

where Σ_ℓ consists of permutations on $\{\epsilon_1, \epsilon_2, \ldots, \epsilon_\ell\}$ while $(\mathbb{Z}/2\mathbb{Z})^\ell$ consists of the sign changes. In particular, the reflection $s_{\epsilon_i - \epsilon_j}$ interchanges ϵ_i and ϵ_j, while s_{ϵ_i} changes the sign on ϵ_i. As in (a), the fundamental reflections $\{s_{\epsilon_1-\epsilon_2}, \ldots, s_{\epsilon_{\ell-1}-\epsilon_\ell}\}$ generate Σ_ℓ. When s_{ϵ_ℓ} (= the sign change on ϵ_ℓ) is also included, we can obtain all sign changes and, hence, the whole group.

Remark: Recall from §3-5 that the reflecting hyperplanes $\{H_{\alpha_1}, \ldots, H_{\alpha_\ell}\}$ of $\{s_{\alpha_1}, \ldots, s_{\alpha_\ell}\}$ are the walls of a Weyl chamber. The above proposition can be reformulated to say that if we choose any Weyl chamber of Δ then W is generated by the reflections having the walls of the chamber as reflecting hyperplanes.

The importance of fundamental reflections goes far beyond the fact that they generate their ambient reflection group. There are many sets of reflections that are not fundamental reflections, but that still generate the reflection group. For example, the permutations $\{(1,2),(1,3),(1,4),\ldots,(1,\ell)\}$ generate Σ_ℓ. Fundamental reflections have additional special properties not possessed by other sets of reflections. The study of length in this chapter, as well as the study of Coxeter systems in Chapter 6, provide extended justifications of this assertion. Almost every result in Chapter 6 depends on the fact that we are using fundamental reflections.

4-2 Length

We now introduce and study the concept of length in an Euclidean reflection group. It will be used in Chapter 6, as an organizing principle; for inductive arguments proving that finite Euclidean reflection groups are Coxeter groups. Let Δ be a root system, and pick a fundamental system Σ of Δ. By Proposition 4-1, $W(\Delta)$ is generated by the fundamental reflections $S = \{s_\alpha \mid \alpha \in \Sigma\}$. Given $\varphi \in W(\Delta)$, the expression of φ in terms of elements from S is typically far from unique. For example, in the dihedral group

$$D_3 = \langle s_1, s_2 \mid (s_1)^2 = (s_2)^2 = (s_1 s_2)^3 = 1\rangle$$

(which is also the symmetric group Σ_3) we have

$$s_1 s_2 = s_2 s_1 s_2 s_1.$$

This raises the question of a minimal expression of φ in terms of S and leads to the concept of the length of φ (with respect to S or, equivalently, with respect to Σ). Given $\varphi \in W(\Delta)$, an expression of φ as a product of n elements from S where n is as small as possible is called a *reduced expression* (or *reduced decomposition*) for φ. (Repetitions of elements from S are allowed and counted as many times as they occur.) It is possible for φ to have different reduced decompositions. For example, in D_3, we have

$$s_1s_2s_1 = s_2s_1s_2.$$

The number of terms in any reduced expression for φ is called the *length of* φ with respect to S. We shall use $\ell(\varphi)$ to denote length. More accurate notation would be $\ell_S(\varphi)$. However, we shall suppress the S and rely on the reader to remember that length is always with respect to a given S (or Σ).

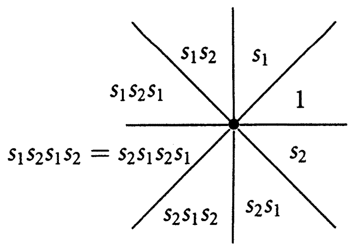
Length satisfies a number of basic properties. For the moment, we shall only emphasize one property.

Lemma $\ell(\varphi^{-1}) = \ell(\varphi)$.

The point is that $\varphi = s_1s_2\cdots s_n$ is a reduced decomposition of φ if and only if $\varphi^{-1} = s_ns_{n-1}\cdots s_1$ is a reduced decomposition of φ^{-1}.

4-3 Length and root systems

Let $W(\Delta)$ be a reflection group with root system Δ. Let Σ be a fundamental system of Δ and let $S = \{s_\alpha \mid \alpha \in \Sigma\}$ be the set of fundamental reflections of $W(\Delta)$ determined by Σ. By §4-1, $W(\Delta)$ is generated by S. In all that follows, we are dealing with expansions of elements of $W(\Delta)$ in terms of the elements of S. As in §4-2, we can define length with respect to S. Recall the diagram



from §1-6, which was meant to suggest that, in the case of the dihedral group D_4, there is a link between length in the group and the action of the group on the chambers and hyperplanes associated with that group. In the next three sections, we shall prove that such a relation actually exists for all reflection groups. The above diagram will be further discussed in §4-5.

Given $\varphi \in W(\Delta)$, we want to explain how expressions of φ in terms of S are related to the action of φ on the root system Δ and on the Weyl chambers of Δ. In particular, we shall relate the length of φ to this action. The use of roots and of chambers represents alternative, but equivalent, approaches to length. In this section and in §4-4 we shall concentrate on the root system approach. In §4-5 we shall discuss the Weyl chamber approach.

Now Σ gives rise to a partition $\Delta = \Delta^+ \coprod \Delta^-$ of Δ into positive and negative roots. Given $\varphi \in W(\Delta)$, let

Definition: $\gamma(\varphi) =$ the number of positive roots transformed by φ into negative roots.

The main result of this section will be:

Theorem A *Given $\varphi \in W(\Delta)$, then $\ell(\varphi) = \gamma(\varphi)$.*

The proof that $\ell(\varphi) = \gamma(\varphi)$ involves a detailed study of the action of $W(\Delta)$ on Δ. We prove Theorem A by obtaining an explicit description of the positive roots which are transformed into negative ones by φ. Given $\varphi \in W(\Delta)$, let

Definition: $\Delta(\varphi) =$ the positive roots transformed by φ into negative roots.

So $\gamma(\varphi) = |\Delta(\varphi)|$. We shall prove

Theorem B *Given $\varphi \in W(\Delta)$, if $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$ is a reduced expression for φ, then*

$$\Delta(\varphi) = \{\alpha_k, s_{\alpha_k} \cdot \alpha_{k-1}, \ldots, (s_{\alpha_k} \cdots s_{\alpha_2}) \cdot \alpha_1\}.$$

The rest of this section will be devoted to the proofs of Theorems A and B. Observe that these theorems are independent. Theorem A is not a corollary of Theorem B, because Theorem A involves the extra assertion that the elements of $\Delta(\varphi)$, listed in Theorem B, are distinct. The proofs of the two theorems will be done simultaneously and will involve a detailed examination of $\Delta(\varphi)$. We proceed using a series of lemmas. Our first lemma is the initial case of Theorems A and B.

Lemma A *Given $\alpha \in \Sigma$, then $\Delta(s_\alpha) = \{\alpha\}$.*

Proof We know that $s_\alpha \cdot \alpha = -\alpha$. So we want to show that $s_\alpha \cdot \beta > 0$ if $\beta > 0$ and $\beta \neq \alpha$. Suppose $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$ and $\alpha = \alpha_i$. Given $\beta > 0$, where $\beta \neq \alpha$, we know that, in the expansion $\beta = \sum \lambda_j \alpha_j$, we must have

$$(*) \qquad \lambda_k > 0 \quad \text{for some } k \neq i.$$

The only other possibility is $\lambda_k = 0$ for all $k \neq i$. Then β is a multiple of $\alpha = \alpha_i$ and, hence, by property (B-1) of root systems, $\beta = \alpha_i$.

It follows from the identity $s_{\alpha_i} \cdot \beta = \beta - \frac{2(\beta,\alpha_i)}{(\alpha_i,\alpha_i)}\alpha_i$ that the only coefficient of β affected by applying s_{α_i} is that of α_i. In particular, it follows from $(*)$ that the coefficient of α_k is positive when we expand $s_{\alpha_i} \cdot \beta$ in terms of Σ. This forces $s_{\alpha_i} \cdot \beta > 0$. ■

Lemma A can be rephrased as stating that, for each $\alpha \in \Sigma$, s_α permutes $\Delta^+ - \{\alpha\}$. It is easy to deduce from this fact that if $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$ then $\gamma(\varphi) \leq k$. It follows that

Corollary A $\gamma(\varphi) \leq \ell(\varphi)$.

The next lemma is concerned with any expression $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$ for φ, reduced or not. Given any such expression, for each $1 \le i \le k$, let

$$\beta_i = (s_{\alpha_k} s_{\alpha_{k-1}} \cdots s_{\alpha_{i+1}}) \cdot \alpha_i.$$

It is possible that there is duplication among the set $\{\beta_i\}$. The next lemma, however, shows that such duplication always leads to a canonical type of cancellation. This type of cancellation is called Matsumoto cancellation and will be further studied in §4-4.

Lemma B *If $\beta_i = \pm\beta_j$ for $i \neq j$, then $\varphi = s_{\alpha_1} \cdots \hat{s}_{\alpha_i} \cdots \hat{s}_{\alpha_j} \cdots s_{\alpha_k}$ (where "^" means "remove").*

Proof Assume that $i < j$. If we take the identity

$$(s_{\alpha_k} s_{\alpha_{k-1}} \cdots s_{\alpha_{i+1}}) \cdot \alpha_i = \pm(s_{\alpha_k} s_{\alpha_{k-1}} \cdots s_{\alpha_{j+1}}) \cdot \alpha_j$$

and cancel, then we have

$$(s_{\alpha_j} s_{\alpha_{j-1}} \cdots s_{\alpha_{i+1}}) \cdot \alpha_i = \pm\alpha_j.$$

In view of property (A-4) in §1-1, plus the fact that $s_\alpha = s_{-\alpha}$, we have

$$s_{\alpha_j} = (s_{\alpha_j} \cdots s_{\alpha_{i+1}}) s_{\alpha_i} (s_{\alpha_{i+1}} \cdots s_{\alpha_j}),$$

which can be rewritten as

$$s_{\alpha_i} s_{\alpha_{i+1}} \cdots s_{\alpha_{j-1}} = s_{\alpha_{i+1}} \cdots s_{\alpha_j}.$$

This equation enables us to transform the expression $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$ into $\varphi = s_{\alpha_1} \cdots \hat{s}_{\alpha_i} \cdots \hat{s}_{\alpha_j} \cdots s_{\alpha_k}$. (Namely, take $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$ and replace $s_{\alpha_i} s_{\alpha_{i+1}} \cdots s_{\alpha_{j-1}}$ by $s_{\alpha_{i+1}} \cdots s_{\alpha_j}$.) ■

In particular, it follows from Lemma B that, when $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$ is a reduced expression for φ, the elements $\{\beta_1, \ldots, \beta_k\}$ are all distinct.

We now set about proving Theorems A and B by induction on $\ell(\varphi)$. The initial case is Lemma A. Assume that $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$ is a reduced expression for $\varphi \in W$. Write $\varphi = \widetilde{\varphi} s_{\alpha_k}$, where $\widetilde{\varphi} = s_{\alpha_1} \cdots s_{\alpha_{k-1}}$ is a reduced expression for $\widetilde{\varphi}$. Assume, by induction, that Theorems A and B hold for $\widetilde{\varphi}$. Let β_i be defined as above. Analogous with this notation, we also let

$$\widetilde{\beta}_i = (s_{\alpha_{k-1}} s_{\alpha_{k-2}} \cdots s_{\alpha_{i+1}}) \cdot \alpha_i$$

for $1 \le i \le k-1$. So we have, for $1 \le i \le k-1$, the relations

$$\beta_i = s_{\alpha_k} \cdot \widetilde{\beta}_i$$
$$\varphi \cdot \beta_i = \widetilde{\varphi} \cdot \widetilde{\beta}_i.$$

Since $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$ is a reduced expression, it follows from Lemma B that the set $\{\beta_1, \ldots, \beta_k\}$ consists of distinct elements. By induction, we have

$$(*) \qquad \Delta(\widetilde{\varphi}) = \{\widetilde{\beta}_1, \ldots, \widetilde{\beta}_{k-1}\}.$$

We know from $(*)$ that $\{\widetilde{\beta}_1, \ldots, \widetilde{\beta}_{k-1}\} \subset \Delta^+$. We can actually prove a stronger result.

Lemma C $\{\widetilde{\beta}_1, \ldots, \widetilde{\beta}_{k-1}\} \subset \Delta^+ - \{\alpha_k\}$.

Proof If $\widetilde{\beta}_i = \alpha_k$, then, applying s_{α_k} to both sides, we obtain $\beta_i = -\alpha_k$. In other words $\beta_i = -\beta_k$ where $i < k$. By Lemma B, we have $\varphi = s_{\alpha_1} \cdots \hat{s}_{\alpha_i} \cdots s_{\alpha_{k-1}} \hat{s}_{\alpha_k}$, which contradicts the fact that $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$ is a reduced expression for φ. ■

In turn, we can use Lemma C to prove:

Lemma D $\{\beta_1, \ldots, \beta_k\} \subset \Delta(\varphi)$.

Proof We have to prove that $\beta_i > 0$ and $\varphi \cdot \beta_i < 0$.

(i) $\beta_i > 0$.

We know that $\beta_k = \alpha_k > 0$. For $i < k$ we have $\beta_i = s_{\alpha_k} \cdot \widetilde{\beta}_i > 0$ because $\widetilde{\beta}_i \in \Delta^+ - \{\alpha_k\}$, and s_{α_k} permutes $\Delta^+ - \{\alpha_k\}$.

(ii) $\varphi \cdot \beta_i < 0$.

We have $\varphi \cdot \beta_k = \widetilde{\varphi} s_{\alpha_k} \cdot \alpha_k = -\widetilde{\varphi} \cdot \alpha_k < 0$. At the last stage, we are using the fact that, by Lemma C, $\alpha_k \notin \Delta(\widetilde{\varphi}) = \{\widetilde{\beta}_1, \ldots, \widetilde{\beta}_{k-1}\}$. In other words, $\widetilde{\varphi} \cdot \alpha_k > 0$. For $i < k$, we have

$$\varphi \cdot \beta_i = \widetilde{\varphi} \cdot \widetilde{\beta}_i < 0. \qquad ■$$

Since the set $\{\beta_1, \ldots, \beta_k\}$ consists of distinct elements, it clearly follows from Lemma D that:

Corollary B $k \leq \gamma(\varphi)$.

We can now easily finish the proof of Theorems A and B. Corollaries A and B give the inequalities

$$k \leq \gamma(\varphi) \leq \ell(\varphi) = k.$$

Thus $\gamma(\varphi) = \ell(\varphi) = k$. So Lemma D can be strengthened to assert that $\{\beta_1, \ldots, \beta_k\} = \Delta(\varphi)$.

4-4 Matsumoto cancellation

By extending the arguments from §4-3, we can prove another important property of reflection groups. This property was already introduced in Lemma 4-3B. It states that a canonical process of cancellation can always be used to turn a nonreduced expression into a reduced one. This cancellation process will play a key role in the proof, to be given in Chapter 6, that finite reflection groups are Coxeter groups.

Let $W(\Delta)$ be a finite Euclidean reflection group with root system Δ. Let Σ be a fundamental system of Δ and let $S = \{s_\alpha \mid \alpha \in \Sigma\}$ be the set of fundamental reflections of $W(\Delta)$ determined by Σ. As in previous sections, we shall be dealing with expansions of elements of $W(\Delta)$ in terms of the elements of S. In particular, length will be defined with respect to S. The rest of this section will be devoted to proving:

***Theorem* (Matsumoto Cancellation Property)** *Given $\varphi \in W(\Delta)$, if $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$ and $\ell(\varphi) < k$, then there exists $1 \leq i < j \leq k$ such that*

$$\varphi = s_{\alpha_1} \cdots \hat{s}_{\alpha_j} \cdots \hat{s}_{\alpha_j} \cdots s_{\alpha_k}.$$

Remark: The cancellation property means that we can delete the terms s_{α_i} and s_{α_j} to obtain an expression for φ involving two fewer terms. So if we start with any expression for φ, we can obtain a reduced expression by cancelling terms in this fashion.

The cancellation property has an equivalent formulation that is also useful. By comparing the two expressions in the above theorem, cancelling, and re-indexing, we can easily obtain:

***Corollary* (Matsumoto Exchange Property)** *Given $\varphi \in W(\Delta)$, if $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$ and $\ell(\varphi) < k$, then there exists $1 \leq i \leq j \leq k$ such that*

$$s_{\alpha_i} \cdots s_{\alpha_j} = s_{\alpha_{i+1}} \cdots s_{\alpha_{j+1}}.$$

In proving Matsumoto cancellation, we shall make use of the sets $\Delta(\varphi)$ introduced in §4-3. Recall that $\ell(\varphi) = |\Delta(\varphi)|$. We shall study the relation between $\Delta(\varphi)$ and $\Delta(\varphi s_\alpha)$ and, hence, between $\ell(\varphi)$ and $\ell(\varphi s_\alpha)$. Our main result in this direction is

Proposition *Given $\varphi \in W(\Delta)$ and $\alpha \in \Sigma$, then $\ell(\varphi s_\alpha) = \ell(\varphi) \pm 1$. Moreover,*

(i) $\ell(\varphi s_\alpha) = \ell(\varphi) + 1$ *if and only if* $\varphi \cdot \alpha > 0$;
(ii) $\ell(\varphi s_\alpha) = \ell(\varphi) - 1$ *if and only if* $\varphi \cdot \alpha < 0$.

We shall first prove this proposition, and then demonstrate how it can be used to prove the Matsumoto cancellation property.

Proof of Proposition Fix $\varphi \in W(\Delta)$ and $\alpha \in \Sigma$. We shall prove the proposition in two steps.

(a) We prove that the two sets $\Delta(\varphi) - \{\alpha\}$ and $\Delta(\varphi s_\alpha) - \{\alpha\}$ have the same cardinality.
(b) We prove that α belongs to either $\Delta(\varphi)$ or $\Delta(\varphi s_a)$, but not both.

Granted the relation between $\ell(\varphi)$ and $\Delta(\varphi)$, and between $\ell(\varphi s_\alpha)$ and $\Delta(\varphi s_\alpha)$, these facts establish the proposition.

Recall that Lemma 4-3A asserts that s_α permutes $\Delta^+ - \{\alpha\}$. We begin the proof of the proposition by showing that, in particular, s_α induces a one-to-one correspondence between $\Delta(\varphi) - \{\alpha\}$ and $\Delta(\varphi s_\alpha) - \{\alpha\}$.

Lemma A $s_\alpha \cdot [\Delta(\varphi) - \{\alpha\}] = \Delta(\varphi s_\alpha) - \{\alpha\}$.

Proof It suffices to show

$$(*) \qquad s_\alpha \cdot [\Delta(\varphi) - \{\alpha\}] \subset \Delta(\varphi s_\alpha) - \{\alpha\};$$

for if we replace φ by φs_α, we obtain

$$s_\alpha \cdot [\Delta(\varphi s_\alpha) - \{\alpha\}] \subset \Delta(\varphi) - \{\alpha\}.$$

Then, applying s_α to both sides, we have the reverse inclusion of $(*)$, namely

$$\Delta(\varphi s_\alpha) - \{\alpha\} \subset s_\alpha \cdot [\Delta(\varphi) - \{\alpha\}].$$

To prove $(*)$, pick $\beta \in \Delta(\varphi) - \{\alpha\}$. So $\beta \in \Delta^+ - \{\alpha\}$ and $\varphi \cdot \beta \in \Delta^-$. We claim that $s_\alpha \cdot \beta \in \Delta(\varphi s_\alpha) - \{\alpha\}$. First of all, by Lemma A, s_α permutes $\Delta^+ - \{\alpha\}$ and, so, $s_\alpha \cdot \beta \in \Delta^+ - \{\alpha\}$. Secondly, $\varphi s_\alpha(s_\alpha \cdot \beta) = \varphi \cdot \beta \in \Delta^-$. ∎

Thus the two sets $\Delta(\varphi) - \{\alpha\}$ and $\Delta(\varphi s_\alpha) - \{\alpha\}$ have the same cardinality. The relation of α to the two sets $\Delta(\varphi)$ and $\Delta(\varphi s_\alpha)$ is given by the following:

Lemma B

(i) $\alpha \in \Delta(\varphi)$ *if and only if* $\varphi \cdot \alpha < 0$;
(ii) $\alpha \in \Delta(\varphi s_\alpha)$ *if and only if* $\varphi \cdot \alpha > 0$.

Proof Since α is a positive root, property (i) is true by definition. For property (ii), we have the equalities

$$\begin{aligned} \alpha \in \Delta(\varphi s_\alpha) &\Leftrightarrow \varphi s_\alpha \cdot \alpha < 0 \\ &\Leftrightarrow \varphi \cdot \alpha = -\varphi s_\alpha \cdot \alpha > 0. \end{aligned}$$ ∎

The proposition easily follows from the above two lemmas.

Proof of Matsumoto Cancellation Property Pick $\varphi \in W(\Delta)$ and an expression $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$ where $\ell(\varphi) < k$. Since $\ell(\varphi) < k$, it follows that, for at least one $j \leq k-1$,

$$\ell(s_{\alpha_1} \cdots s_{\alpha_{j+1}}) = \ell(s_{\alpha_1} \cdots s_{\alpha_j}) - 1.$$

By the above proposition, this equality is the same as asserting that

$$(s_{\alpha_1} \cdots s_{\alpha_j}) \cdot \alpha_{j+1} < 0.$$

Choose $i \leq j$ such that

$$(s_{\alpha_{i+1}} \cdots s_{\alpha_j}) \cdot \alpha_{j+1} > 0$$

$$(s_{\alpha_i} s_{\alpha_{i+1}} \cdots s_{\alpha_j}) \cdot \alpha_{j+1} < 0.$$

Since s_{α_i} permutes $\Delta^+ - \{\alpha_i\}$, we must have

$$(s_{\alpha_{i+1}} \cdots s_{\alpha_j}) \cdot \alpha_{j+1} = \alpha_i.$$

In view of property (A-4) in §1-1, we have

$$s_{\alpha_i} = (s_{\alpha_{i+1}} \cdots s_{\alpha_j}) s_{\alpha_{j+1}} (s_{\alpha_j} \cdots s_{\alpha_{i+1}}),$$

which can be rewritten as

$$s_{\alpha_i} s_{\alpha_{i+1}} \cdots s_{\alpha_j} = s_{\alpha_{i+1}} \cdots s_{\alpha_{j+1}}.$$

This equality enables us to transform the expression $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$ into the form $\varphi = s_{\alpha_1} \cdots \hat{s}_{\alpha_i} \cdots \hat{s}_{\alpha_{j+1}} \cdots s_{\alpha_k}$. ∎

4-5 Length and reflecting hyperplanes

In this section, we explain how the characterization of length in terms of root systems, as given in §4-3, can be reformulated in terms of reflecting hyperplanes and their associated chamber system. We shall demonstrate that the diagram from §4-3 for the dihedral group D_4 actually illustrates a general situation.

Let Δ, $W(\Delta)$, Σ and S be as in §4-3. The reflecting hyperplanes of $W(\Delta)$ consist of the set $\{H_\alpha \mid \alpha \in \Delta^+\}$. A reflecting hyperplane H_α *separates* two chambers $\mathcal{C}_1$ and $\mathcal{C}_2$ if they lie on opposite sides of H_α. In other words, for any $t_1 \in \mathcal{C}_1$ and $t_2 \in \mathcal{C}_2$, the signs of (α, t_1) and (α, t_2) are opposite. Let $\mathcal{C}_o$ be the fundamental chamber with respect to Σ as discussed in §3-5, i.e.,

$$\mathcal{C}_o = \{t \in \mathbb{E} \mid (t, \alpha) > 0 \text{ for } \alpha \in \Sigma\}.$$

$W(\Delta)$ acts on the set of chambers. The action follows from the fact that $W(\Delta)$ permutes the reflection hyperplanes (by the rule $\varphi \cdot H_\alpha = H_{\varphi \cdot \alpha}$) and, so, $W(\Delta)$ also permutes the connected components of $\mathbb{E} - (\bigcup_{\alpha \in \Delta} H_\alpha)$. Given $\varphi \in W(\Delta)$, let

Definition: $\lambda(\varphi) =$ the number of reflecting hyperplanes separating $\mathcal{C}_o$ and $\varphi \cdot \mathcal{C}_o$.

We shall prove:

Theorem *Given $\varphi \in W(\Delta)$, then $\ell(\varphi) = \lambda(\varphi)$.*

Proof In view of Lemma 4-2 and Theorem 4-3A, we have the equalities $\ell(\varphi) = \ell(\varphi^{-1}) = \gamma(\varphi^{-1})$. So it suffices to show

$$\gamma(\varphi^{-1}) = \lambda(\varphi).$$

Since $H_\alpha = H_{-\alpha}$ for each $\alpha > 0$, we can index the reflecting hyperplanes by the positive roots. The above identity now follows from the fact that, for any $\alpha > 0$ and $t \in \mathcal{C}_o$, we have the equivalences

$$\begin{aligned} H_\alpha \text{ separates } \mathcal{C}_o \text{ and } \varphi \cdot \mathcal{C}_o &\Leftrightarrow (\varphi \cdot t, \alpha) < 0 \\ &\Leftrightarrow (t, \varphi^{-1} \cdot \alpha) < 0 \\ &\Leftrightarrow \varphi^{-1} \cdot \alpha < 0. \end{aligned}$$

For the last equivalence, we are using the fact that the negative roots with respect to Σ are determined by being negative when evaluated on the chamber ($= \mathcal{C}_o$) corresponding to Σ. ■

4-6 The action of $W(\Delta)$ on fundamental systems and Weyl chambers

In this section, we give an application of our characterizations of length. We explain how the one-to-one correspondence in §3-5 can be extended to

$$\{\text{chambers}\} \leftrightarrow \{\text{fundamental systems}\} \leftrightarrow W(\Delta).$$

Theorem 4-5 will play a central role in this discussion. First of all, observe that $W(\Delta)$ acts both on the set of chambers and on the set of fundamental systems. The action on the chambers was discussed in §4-5. The action on the fundamental systems is induced by the action of $W(\Delta)$ on Δ. Secondly, observe that the one-to-one correspondence

$$\{\text{chambers}\} \leftrightarrow \{\text{fundamental systems}\}$$

is actually equivariant with respect to the action of $W(\Delta)$ on the two sets. (We use the identity $(\varphi \cdot t, \varphi \cdot \alpha_i) = (t, \alpha_i)$ to show this).

In the rest of this section, it will be shown that $W(\Delta)$ acts freely and transitively on $\{\text{chambers}\} = \{\text{fundamental systems}\}$. In particular, this will establish the desired one-to-one correspondence between these two sets. The freeness and the transitivity of the $W(\Delta)$ action will be analyzed in two different propositions.

Proposition A *$W(\Delta)$ acts transitively on the Weyl chambers of Δ.*

Proof Pick a fundamental system $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$. Then

$$\mathcal{C}_o = \{t \in \mathbb{E} \mid (t, \alpha_i) > 0 \; i = 1, \ldots, \ell\}$$

is the corresponding fundamental chamber. Given a chamber $\mathcal{C}$, we want to show that there exists $\varphi \in W(\Delta)$ so that $\varphi\cdot\mathcal{C} = \mathcal{C}_o$. It suffices to show that $(\varphi\cdot\mathcal{C})\cap\mathcal{C}_o \neq \varnothing$ for some $\varphi \in W$. In turn, let

$$\overline{\mathcal{C}_o} = \{t \in \mathbb{E} \mid (t, \alpha_i) \geq 0 \; i = 1, \ldots, \ell\}$$

be the closure of $\mathcal{C}_o$. It suffices to prove that $\varphi \cdot \mathcal{C} \cap \overline{\mathcal{C}_o} \neq \varnothing$ for some $\varphi \in W$, because $\overline{\mathcal{C}_o} - \mathcal{C}_0$ lies in $\bigcup_{\alpha\in\Delta} H_\alpha$ and $(\bigcup_{\alpha\in\Delta} H_\alpha) \cap (\varphi \cdot \mathcal{C}) = \varnothing$. Pick $a \in \mathcal{C}$ and let

$$\Gamma = \text{the } W \text{ orbit of } a \text{ in } \mathbb{E}.$$

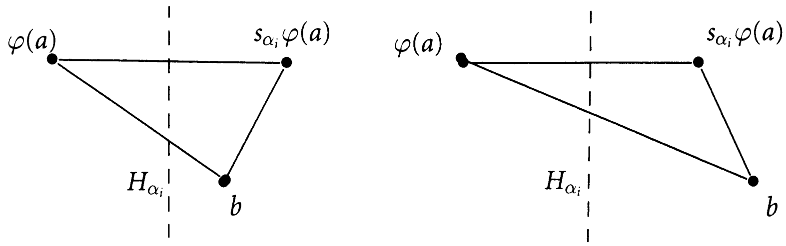
To show $\overline{\mathcal{C}_o} \cap \Gamma \neq \varnothing$, pick $b \in \mathcal{C}_o$ and consider

$$d = \min\{\|b - x\| \mid x \in \Gamma\}.$$

Pick $\varphi \cdot a \in \Gamma$ such that $d = \|b - \varphi \cdot a\|$. We claim $\varphi \cdot a \in \overline{\mathcal{C}_o}$. If not, then $(\varphi \cdot a, \alpha_i) < 0$ for some α_i. So $\varphi \cdot a$ and b lie on opposite sides of the hyperplane H_{α_i}. It is easy to see that

$$\|s_{\alpha_i}\varphi \cdot a - b\| < \|\varphi \cdot a - b\|.$$

The following pictures illustrate the possibilities.



(The dashed line denotes the reflecting hyperplane H_{α_i} of s_{α_i}.) The following manipulation verifies these pictures.

$$\begin{aligned}
\|s_{\alpha_i}\varphi \cdot a - b\|^2 &= (s_{\alpha_i}\varphi \cdot a - b, s_{\alpha_i}\varphi \cdot a - b) \\
&= (s_{\alpha_i}\varphi \cdot a, s_{\alpha_i}\varphi \cdot a) - 2(s_{\alpha_i}\varphi \cdot a, b) + (b, b) \\
&= (\varphi \cdot a, \varphi \cdot a) - 2\left(\varphi \cdot a - 2\frac{(\varphi \cdot a, \alpha_i)}{(\alpha_i, \alpha_i)}\alpha_i, b\right) + (b, b) \\
&= (\varphi \cdot a, \varphi \cdot a) - 2(\varphi \cdot a, b) + (b, b) + 4\frac{(\varphi \cdot a, \alpha_i)}{(\alpha_i, \alpha_i)}(\alpha_i, b) \\
&= \|\varphi \cdot a - b\|^2 + 4\frac{(\varphi \cdot a, \alpha_i)}{(\alpha_i, \alpha_i)}(\alpha_i, b) \\
&< \|\varphi \cdot a - b\|^2.
\end{aligned}$$

The last inequality is based on the inequalities $(\varphi \cdot a, \alpha_i) < 0$, $(\alpha_i, \alpha_i) > 0$ and $(\alpha_i, b) > 0$ ($b \in \mathcal{C}_0$!). So we have contradicted the fact that $d = \|\varphi \cdot a - b\|$. ■

Secondly, it is a trivial consequence of the characterizations of length in §4-5 that

Proposition B *$W(\Delta)$ acts freely on the Weyl chambers of Δ.*

Proof In view of Proposition A, it suffices to show that no element of $W(\Delta)$ fixes the fundamental chamber. Given $\varphi \in W(\Delta)$, if φ fixes the fundamental chamber then by Theorem 4-5 $\ell(\varphi) = \lambda(\varphi) = 0$. So $\varphi = 1$. ∎

We record for use in §5-2 a consequence of the argument used to prove Proposition A.

Corollary **(of proof)** *Every W orbit in $\mathbb{E}$ intersects $\overline{\mathcal{C}_o}$, i.e., $\mathbb{E} = \bigcup_{\varphi \in W} \varphi \cdot \overline{\mathcal{C}_o}$.*

5 Parabolic subgroups

The material in this chapter is not really needed until the study of conjugacy classes in Chapters 27–30. However, it is introduced at this time because it is a natural extension of the ideas discussed in previous chapters, particularly the results of Chapter 4. Let $W \subset O(\mathbb{E})$ be a finite Euclidean reflection group. In Chapter 4 we studied the interaction between the algebraic structure of W and its action on $\mathbb{E}$. Parabolic subgroups arise naturally out of that discussion. Parabolic subgroups and subroot systems will be introduced in §5-1. In §5-2 it will be shown that parabolic subgroups are the isotopy groups of the action of W on $\mathbb{E}$. This fact is a generalization of the fact that W acts freely on the Weyl chambers. The last two sections, §5-3 and §5-4, are devoted to the effect of conjugation on parabolic subgroups of reflection groups. This theme will be explored again in Chapter 28.

5-1 Parabolic subgroups

Let $W = W(\Delta)$ be a finite Euclidean reflection group with root system $\Delta \subset \mathbb{E}$. Let $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$ be a fundamental system for Δ. So W is generated by the fundamental reflections $S = \{s_{\alpha_1}, \ldots, s_{\alpha_\ell}\}$. Given $I \subset \{1, 2, \ldots, \ell\}$, let

$$W_I = \text{the subgroup of } W \text{ generated by } \{s_{\alpha_i} \mid i \in I\}.$$

Such a subgroup is called a *parabolic subgroup* of W. This defines parabolic subgroups with respect to Σ. To obtain the complete collection of parabolic subgroups, we must consider those defined with respect to all fundamental systems of Δ.

If we fix a particular fundamental system Σ, then every parabolic subgroup is conjugate to a parabolic subgroup with respect to Σ; for, given another fundamental system Σ', then $\varphi \cdot \Sigma = \Sigma'$ for some $\varphi \in W$ (see Proposition 4-6A) and the inner automorphism $\varphi\_\varphi^{-1}\colon W \to W$ maps the fundamental reflections $S = \{s_\alpha \mid \alpha \in \Sigma\}$ to the fundamental reflections $S' = \{s_{\alpha'} \mid \alpha' \in \Sigma'\}$ (see property (A-4) of §1-1). Thus the parabolic subgroups of W defined using Σ are conjugate to those defined using Σ'.

There are further conjugacy relations between parabolic subgroups. If we fix Σ and look at the different parabolic subgroups defined using a fixed Σ, then they are sometimes conjugate to each other. This topic is, however, more complicated. These extra conjugations will be initially discussed in §5-3 and then analyzed in more detail in Chapter 28.

Besides parabolic subgroups we can also define *parabolic subroot systems*. For each $I \subset \{1, 2, \ldots, \ell\}$, let

$$\Sigma_I = \{\alpha_i \mid i \in I\}$$

$$\Delta_I = \text{the subroot system generated by } \Sigma_I.$$

Then Σ_I is a fundamental system for Δ_I. There is an obvious relation between parabolic subgroups and parabolic subroot systems: namely, W_I is the reflection group associated to the root system Δ_I and we can write $W = W(\Delta_I)$.

Example: In the case of the root system $\Delta = A_\ell$, the parabolic subroot systems are disjoint unions of the form $A_{i_1} \coprod \cdots \coprod A_{i_k}$, while the parabolic subgroups of $W(A_\ell) = \Sigma_{\ell+1}$ consist of products of the form $\Sigma_{i_1+1} \times \cdots \times \Sigma_{i_k+1}$.

This example is not too hard to see, even at this stage. But the determination of parabolic subroot systems and subgroups for a general Δ and $W(\Delta)$ clearly requires better techniques of analysis. This will be provided once Coxeter systems have been introduced and studied in Chapters 6–8. Coxeter graphs provide a heuristic device for the study of fundamental systems and, therefore, of parabolics. For example, the Borel-de Siebenthal Theorem of Chapter 12 is a clear example of the efficacy of such graphs in analyzing crystallographic subroot systems. In the rest of this chapter, however, we shall be studying parabolic subgroups without introducing Coxeter graphs.

The transitivity of the parabolic relation (for groups as well as root systems) follows from:

Lemma A *If $\Delta'' \subset \Delta'$, and $\Delta' \subset \Delta$ are parabolic subroot systems, then $\Delta'' \subset \Delta$ is a parabolic subroot system as well.*

Proof Pick fundamental systems $\Sigma \subset \Delta$ and $\Sigma' \subset \Delta'$ and inclusions

$$\Sigma_I \subset \Sigma \quad \text{and} \quad \Sigma'_J \subset \Sigma'$$

realizing $\Delta' \subset \Delta$ and $\Delta'' \subset \Delta'$ as parabolic subroot systems, i.e.,

$$\Delta' = \Delta_I \quad \text{and} \quad \Delta'' = \Delta'_J.$$

Since both Σ' and Σ_I are fundamental systems of Δ', we can choose $\varphi \in W' = W(\Delta')$ such that $\Sigma' = \varphi \cdot \Sigma_I$. But then

$$\Sigma'_J \subset \Sigma' = \varphi \cdot \Sigma_I \subset \varphi \cdot \Sigma,$$

which verifies that $\Delta'' \subset \Delta$ is a parabolic subroot system. ■

As explained in §4-2, we can define length in $W(\Delta)$ with respect to each fundamental system. If we make the appropriate choices, then there is compatibility between length in a reflection group and in its parabolic subgroups. Let Σ be a fundamental system for the root system Δ. Given $I \subset \{1, \ldots, \ell\}$, let $\Sigma_I \subset \Sigma$ be the fundamental system for the parabolic subroot system $\Delta_I \subset \Delta$. Given $\varphi \in W_I \subset W$, let

$$\ell(\varphi) = \text{length in } W \text{ with respect to } \Sigma$$
$$\ell_I(\varphi) = \text{length in } W_I \text{ with respect to } \Sigma_I.$$

Lemma B *For any $\varphi \in W_I$, $\ell_I(\varphi) = \ell(\varphi)$.*

Proof Let
$$\Delta = \Delta^+ \coprod \Delta^-$$
be the decomposition of Δ into positive and negative roots with respect to Σ, and let
$$\Delta_I = \Delta_I^+ \coprod \Delta_I^-$$
be the decomposition of Δ_I into positive and negative roots with respect to Σ_I. This second decomposition is obtained by restricting the first decomposition $\Delta = \Delta^+ \coprod \Delta^-$ to Δ_I. It was shown in §4-3 that the length of any $\varphi \in W$ can be determined from its action on the root system Δ. If we let

$$\Delta(\varphi) = \text{the positive roots of } \Delta, \text{ which } \varphi \text{ converts into negative roots,}$$

then Theorem 4-3A asserts that

$$\ell(\varphi) = |\Delta(\varphi)|.$$

After defining analogues to the above, we have, for any $\varphi \in W_I$, the identity

$$\ell_I(\varphi) = |\Delta_I(\varphi)|.$$

And, given $\varphi \in W_I$, we then have the inequalities

$$\ell(\varphi) \leq \ell_I(\varphi) = |\Delta_I(\varphi)| \leq |\Delta(\varphi)| = \ell(\varphi).$$

Thus we must have $\ell(\varphi) = \ell_I(\varphi)$. ■

We end this section by discussing coset representatives for W_I. Let

$$\begin{aligned} W^I &= \{\varphi \in W \mid \varphi \cdot \alpha_i > 0 \text{ for } i \in I\} \\ &= \{\varphi \in W \mid \ell(\varphi s_{\alpha_i}) = \ell(\varphi) + 1 \text{ for } i \in I\}. \end{aligned}$$

The equivalence of the two different conditions used to describe W^I is provided by Proposition 4-4. We shall prove that the set W^I provides coset representatives for W_I, i.e., $W = W^I W_I$.

Lemma C *Every $\varphi \in W$ can be decomposed $\varphi = \varphi^I \varphi_I$, where $\varphi^I \in W^I$, $\varphi_I \in W_I$.*

Proof By induction on length. We can assume $\varphi \notin W^I$. It follows, from the above description of W^I and from Proposition 4-4, that there exists $i \in I$ such that
$$\ell(\varphi s_{\alpha_i}) = \ell(\varphi) - 1.$$
By induction, $\varphi s_{\alpha_i} = \varphi^I \varphi_I$, where $\varphi^I \in W^I$, $\varphi_I \in W_I$. So
$$\varphi = (\varphi^I)(\varphi_I s_{\alpha_i}).$$
This decomposition is of the desired form. ■

Remark: With more work, we can show that the decomposition $\varphi = \varphi^I \varphi_I$ is unique and that $\ell(\varphi) = \ell(\varphi^I) + \ell(\varphi_I)$. Moreover, the element φ^I can be characterized as the element of minimal length in the coset φW_I.

5-2 Isotropy subgroups

In this section, we show how parabolic subgroups arise naturally when we consider the action of W on $\mathbb{E}$.

Definition: Given a set $\Gamma \subset \mathbb{E}$, the *isotropy group* of Γ is

$$W_\Gamma = \{\varphi \in W \mid \varphi \cdot x = x \text{ for all } x \in \Gamma\}.$$

The main result of this section is:

Theorem *For any set $\Gamma \subset \mathbb{E}$, $W_\Gamma \subset W$ is a parabolic subgroup.*

Since parabolic subgroups are, by definition, reflection subgroups, we also have

Corollary *For any set $\Gamma \subset \mathbb{E}$, $W_\Gamma \subset W$ is a reflection subgroup.*

Most of the remainder of this section will be devoted to the proof of the above theorem. Before giving the proof, we first study the fundamental chamber of a reflection group and its relation to isotropy subgroups. As in §4-5 and §4-6, pick a fundamental system $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$ and let

$$\mathcal{C}_o = \{t \in \mathbb{E} \mid (\alpha_i, t) > 0\}$$

be the fundamental Weyl chamber determined by Σ. The closure of $\mathcal{C}_o$ is

$$\overline{\mathcal{C}_o} = \{t \in \mathbb{E} \mid (\alpha_i, t) \geq 0\}.$$

There is a canonical decomposition of $\mathcal{C}_o$. Given $I \subset \{1, 2, \ldots, \ell\}$, let

$$\mathcal{C}_I = \left\{ t \in \mathbb{E} \;\middle|\; \begin{matrix} (t, \alpha_i) = 0 \text{ for } i \in I \\ (t, \alpha_i) > 0 \text{ for } i \notin I \end{matrix} \right\}.$$

Each $\mathcal{C}_I$ is a *convex cone*, i.e., closed under addition and multiplication by positive scalars. Each $\mathcal{C}_I$ is also a *cell*, i.e., homeomorphic to an open ball. In particular, $\mathcal{C}_\varnothing = \mathcal{C}_o$, the fundamental chamber. We shall continue to use the symbol $\mathcal{C}_o$ (rather than $\mathcal{C}_\varnothing$) for this case. We have a disjoint union

$$\overline{\mathcal{C}_o} = \coprod_I \mathcal{C}_I.$$

The parabolic subgroups $\{W_I\}$ associated with Σ have a very nice relation with this cellular decomposition.

Proposition A *Given $I \subset \{1, 2, \ldots, \ell\}$, then W_I is the isotropy group of each $x \in \mathcal{C}_I$.*

Obviously, $W_I \subset$ the isotropy group of $\mathcal{C}_I$. The method of obtaining equality is to use the canonical representatives W^I for the cosets W/W_I, which were discussed in §5-1. These coset representatives have the property that all of them, except $\varphi = 1$, act on $\mathcal{C}_I$ in a highly nontrivial manner.

Lemma *Given $1 \neq \varphi \in W^I$, then $(\varphi \cdot \mathcal{C}_I) \cap \overline{\mathcal{C}_o} = \phi$.*

Proof First of all, $\varphi \neq 1$ implies that $\varphi \cdot \alpha_i < 0$ for some $1 \leq i \leq \ell$. Since $\varphi \in W^I$, we also have $i \notin I$. Now, pick $x \in \mathcal{C}_I$. Since $i \notin I$, we have $(x, \alpha_i) > 0$. Thus

$$(\varphi \cdot x, \varphi \cdot \alpha_i) > 0.$$

We now show that $\varphi \cdot x \in \overline{\mathcal{C}_o}$ produces a contradiction to this inequality. Since $\varphi \cdot \alpha_i < 0$, we have $(y, \varphi \cdot \alpha_i) < 0$ for all $y \in \mathcal{C}_o$. So $(y, \varphi \cdot \alpha_i) \leq 0$ for all $y \in \overline{\mathcal{C}_o}$. In particular, $\varphi \cdot x \in \overline{\mathcal{C}_o}$ implies

$$(\varphi \cdot x, \varphi \cdot \alpha_i) \leq 0. \qquad \blacksquare$$

The proposition easily follows. Pick $\varphi \in W$. Then we can decompose $\varphi = \varphi^I \varphi_I$, where $\varphi^I \in W^I$ and $\varphi_I \in W_I$. So $\varphi \in W_I$ if and only if $\varphi^I = 1$. On the other hand,

$$\varphi \cdot \mathcal{C}_I = \varphi^I \varphi_I \cdot \mathcal{C}_I = \varphi^I \cdot \mathcal{C}_I.$$

So $(\varphi \cdot \mathcal{C}_I) \cap \overline{\mathcal{C}_o} \neq \varnothing$ if and only if $\varphi^I = 1$. This finishes the proof of the proposition.

Proof of Theorem We prove the theorem by reducing it to Proposition A. We need only prove a very special case of the theorem in order to deduce the general result. That is, we can reduce the proof of the theorem to the case where

$$\Gamma = \{x\},$$

i.e., Γ is a set consisting of a single element. We can reduce to the case of Γ being finite by using linearity. The reduction to Γ being a single point follows by an inductive argument on $|\Gamma|$. We decompose $\Gamma = \Gamma' \coprod \{x\}$ and use the relation $W_\Gamma = (W_x)_{\Gamma'}$. We also need to use the fact, demonstrated in §5-1, that the relation of being a parabolic subgroup is a transitive one. That is, if we prove that $W_x \subset W$ and $(W_x)_{\Gamma'} \subset W_x$ are parabolic subgroups, then it follows that $(W_x)_{\Gamma'} \subset W$ is a parabolic subgroup as well.

Next, in studying the isotropy groups W_x of a point $x \in \mathbb{E}$, we need only consider very special cases of $x \in \mathbb{E}$. It suffices to assume that

$$x \in \overline{\mathcal{C}_o}$$

because Corollary 4-6 implies that $x = \varphi \cdot y$ for some $y \in \overline{\mathcal{C}_o}$. If $x = \varphi \cdot y$, then $W_x = \varphi W_y \varphi^{-1}$. So if W_y is a parabolic subgroup with respect to Σ, then W_x is a parabolic subgroup with respect to the fundamental system $\Sigma' = \varphi \cdot \Sigma$.

Thus we are reduced to showing that W_x is a parabolic subgroup with respect to Σ for each $x \in \overline{\mathcal{C}_o}$. Proposition A now clearly suffices to establish the theorem.

Remark 1: The *rank* of a reflection group W is the rank of any root system of W, i.e., the number of roots in any fundamental system. We can easily use this argument to produce a strengthened version of the above theorem. Proposition A not only shows that the isotropy group of a subset $S \subset \mathbb{E}$ is a reflection group, but

also that, if $S \neq \varnothing$, then the isotropy group of Γ has rank smaller than that of W. We shall use this fact in §30-1 for an inductive argument.

Decomposition of $\mathbb{E}$ We can use the action of W on $\mathbb{E}$ to extend the decomposition $\overline{\mathcal{C}_o} = \coprod_I \mathcal{C}_I$ from $\overline{\mathcal{C}_o}$ to all of $\mathbb{E}$. In the process, we also demonstrate that $\overline{\mathcal{C}_o}$ is a *fundamental domain* for the action of W on $\mathbb{E}$, i.e., each W orbit of $\mathbb{E}$ intersects $\overline{\mathcal{C}_o}$ in an unique point. The key fact used is the existence of a set of coset representatives for W/W_I, with the properties described in the above lemma. In view of Proposition A, we have well-defined maps:

$$(W/W_I) \times \mathcal{C}_I \longrightarrow \mathbb{E}$$

$$(\varphi W_I,) \longmapsto \varphi \cdot x.$$

This map is surjective because we know from Corollary 4-6 that each W orbit of $\mathbb{E}$ intersects $\overline{\mathcal{C}_o}$ in some point, i.e.,

$$\mathbb{E} = \bigcup_{\varphi \in W} \varphi \cdot \overline{\mathcal{C}_o}.$$

Granted the existence of coset representatives for W/W_I such that $(\varphi \cdot \mathcal{C}_I) \cap \overline{\mathcal{C}_o} = \varnothing$ whenever $\varphi \neq 1$, this map actually provides a decomposition of $\mathbb{E}$.

Proposition B $\mathbb{E} = \coprod_I (W/W_I) \times \mathcal{C}_I$, *where I ranges over the subsets of* $\{1, 2, \ldots, \ell\}$.

We have obtained a decomposition of $\mathbb{E}$ into the disjoint pieces

$$\{\varphi \cdot \mathcal{C}_I \mid I \subset \{1, \ldots, \ell\} \text{ and } \varphi \in W/W_I\}.$$

Each $\varphi \cdot \mathcal{C}_I$ is a convex cone and also a cell. By definition, the action of W on $\mathbb{E}$ respects the decomposition of $\mathbb{E}$ into cells. And the action of W on $\mathbb{E}$ is being used to extend the decomposition of $\overline{\mathcal{C}_o}$ given by $\coprod_I \mathcal{C}_I$ to all of $\mathbb{E}$. In particular, $\overline{\mathcal{C}_o} = \coprod_I \mathcal{C}_I$ is a fundamental domain for the action.

Remark 2: The above cells in $\mathbb{E}$ are also determined by introducing, for each $\alpha \in \Delta$, one of the three restraints:

$$(\alpha, x) = 0 \quad \text{or} \quad (\alpha, x) > 0 \quad \text{or} \quad (\alpha, x) < 0.$$

For some choices, we obtain the empty set ϕ. The nontrivial cases, however, decompose $\mathbb{E}$ into disjoint subsets and are the various cells $\{\varphi \cdot \mathcal{C}_I\}$ of $\mathbb{E}$.

To verify this assertion, we begin by observing that each of the $\mathcal{C}_I$ is clearly determined by a choice of such constraints. Since $(\varphi \cdot x, \varphi \cdot y) = (x, y)$, it follows that a set of such constraints determines each cell $\varphi \cdot \mathcal{C}_I$. Finally, since both the cells and the sets determined by constraints decompose $\mathbb{E}$, it follows that every nontrivial set determined by constraints must be a cell. This alternative characterization of the cells $\{\varphi \cdot \mathcal{C}_I\}$ will be used in the proof of Proposition 27-4.

5-3 Conjugation of parabolic subgroups

The question of classifying parabolic subgroups up to conjugacy will be briefly discussed in this section (and in more detail in Chapter 28). Let W be a finite Euclidean reflection group with associated root system Δ. Let $\Sigma = \{\alpha_1, \dots, \alpha_\ell\}$ be a fundamental system for Δ. In studying conjugacy classes of parabolic subgroups, we are reduced to studying the parabolic subgroups defined with respect to Σ, because every parabolic subgroup is conjugate to a parabolic subgroup defined with respect to Σ. Given $I \subset \{1, 2, \dots, \ell\}$, then, as in §5-1, let

$$\Sigma_I = \{\alpha_i \mid i \in I\}$$
$$\Delta_I = \text{the subroot system generated by } \Sigma_I$$
$$W_I = W(\Delta_I).$$

We want to determine all the possibilities for W_I and, also, when two of them are conjugate to each other. It was already suggested in §5-1 that the possibilities for W_I are determinable, and that this process will become considerably easier once the machinery of Coxeter graphs is introduced. So this section will be focusing on the second question, i.e., when can W_I and W_I be conjugate to each other.

Two subsets S and S' of $\mathbb{E}$ are *W-equivalent* if there exists $\varphi \in W$ so that $\varphi \cdot S = S'$. The question of W_I and W_J being conjugate in W reduces to the question of such W equivalences, since we have

Proposition *Given $I, J \subset \{1, \dots, \ell\}$, then the following are equivalent:*

(i) W_I and W_J are conjugate in W;
(ii) Δ_I and Δ_J are W-equivalent;
(iii) Σ_I and Σ_J are W-equivalent.

Proof First of all, (i) and (ii) are equivalent. This follows from property (A-4) of §1-1, and the identities $W_I = W(\Delta_I)$ and $W_J = W(\Delta_J)$. Secondly, (ii) and (iii) are equivalent. We use the fact that Σ_I and Σ_J are fundamental systems for Δ_I and Δ_J. Clearly, (iii) implies (ii). Conversely, suppose $\varphi \cdot \Delta_I = \Delta_J$. Then $\varphi \cdot \Sigma_I$ is a fundamental system of $\varphi \cdot \Delta_I = \Delta_J$. Since W_J acts transitively on the fundamental systems of Δ_J (see §4-6), it follows that $\varphi \cdot \Sigma_I$ and Σ_J are related by some $\varphi' \in W_J$, i.e., $(\varphi'\varphi) \cdot \Sigma_I = \Sigma_J$.

In Chapter 28, a technical condition will be obtained for determining when Σ_I and Σ_J can be W-equivalent. This technical condition, when combined with the above proposition, will reduce the study of conjugacy of parabolics in W to an analysis of the Coxeter graph of W.

II Coxeter groups

In the next three chapters, we shall discuss the algebraic structure of reflection groups. The main concepts are Coxeter systems and Coxeter groups. A Coxeter system is a special type of group presentation possessed by every finite Euclidean reflection group. The goal of the next three chapters is to study and classify finite Coxeter systems and finite reflection groups. One of the main themes of this study will be that the algebraic structure of a finite reflection group (namely, its Coxeter system) arises from, and mirrors, precise facts about the geometry of the reflection group (namely, its configuration of reflecting hyperplanes).

In Chapter 6, we introduce Coxeter systems and Coxeter groups, and demonstrate that every finite reflection group has a canonical Coxeter system associated to it. In Chapter 7 we introduce the bilinear form of a Coxeter system, and prove that this bilinear form is always positive definite when the Coxeter system is finite. In Chapter 8 we work out the classification of finite Coxeter systems and finite Euclidean reflection groups.

6 Reflection groups and Coxeter systems

In this chapter, we shall explain how the algebraic structure of finite Euclidean reflection groups can be captured in the concept of a Coxeter system. In the next two chapters, we use this algebraic structure to classify finite reflection groups.

6-1 Coxeter groups and Coxeter systems

The basic algebraic structure used to understand finite Euclidean reflection groups is the concept of a Coxeter group. We have already introduced in §1-3 the idea of a presentation $G = \langle S \mid R \rangle$ of a group G. A Coxeter group is a group possessing a canonical presentation called a Coxeter system. As we shall see, the presentation of the dihedral group given in §1-3 is the simplest example of a Coxeter system. A dihedral group is a Coxeter group and, conversely, we can say that a Coxeter group is a generalized dihedral group.

Definition: A group W is a *Coxeter group* if there exists $S \subset W$ such that

$$W = \langle s \in S \mid (ss')^{m_{ss'}} = 1 \rangle,$$

where

$$m_{ss} = 1 \quad \text{and} \quad m_{ss'} \in \{2, 3, \dots\} \cup \{\infty\} \quad \text{if } s \neq s'.$$

In particular, the relations $m_{ss} = 1$ assert that each s is an involution. In §7-2 we shall show that $m_{ss'}$ is actually the order of ss'. We shall do so by constructing a representation (the Tits representation) of the Coxeter group where, for each s and s', ss' is a rotation of order $m_{ss'}$. Notice that

$$m_{ss'} = 2 \Leftrightarrow ss'ss' = 1 \Leftrightarrow ss' = s's.$$

So we can view the integers $m_{ss'} \geq 3$ as expressing, in a systematic way, the lack of commutativity in W.

The pair (W, S) is called a *Coxeter system.* We shall be interested in *finite Coxeter systems,* namely those for which W is finite. We shall say that (W, S) and (W', S') are *isomorphic* if there is a group isomorphism $W \rightarrow W'$ sending S to S'. The Coxeter system has *rank* ℓ if $|S| = \ell$. The Coxeter system (W, S) is *reducible* if $W = W_1 \times W_2$ and $S = S_1 \coprod S_2$, where $\varnothing \neq S_1 \subset W_1$, $\varnothing \neq S_2 \subset W_2$ and (W_1, S_1), (W_2, S_2) are Coxeter systems. Otherwise, the Coxeter system is said to be *irreducible.*

We have already seen examples of Coxeter systems in Chapter 1. The presentation

$$D_n = \langle s_1, s_2 \mid (s_1)^2 = (s_2)^2 = (s_1 s_2)^n = 1 \rangle$$

of the dihedral group given in Proposition 1-3B is the simplest example of a Coxeter presentation. In addition, it was suggested (but not proven) in §1-6 that the

automorphism groups of the tetrahedron, cube and dodecahedron are given by the following three descriptions:

$$\langle s_1, s_2, s_3 \mid (s_1)^2 = (s_2)^2 = (s_3)^2 = (s_1 s_3)^2 = (s_1 s_2)^3 = (s_2 s_3)^3 = 1\rangle$$
$$\langle s_1, s_2, s_3 \mid (s_1)^2 = (s_2)^2 = (s_3)^2 = (s_1 s_3)^2 = (s_1 s_2)^3 = (s_2 s_3)^4 = 1\rangle$$
$$\langle s_1, s_2, s_3 \mid (s_1)^2 = (s_2)^2 = (s_3)^2 = (s_1 s_3)^2 = (s_1 s_2)^3 = (s_2 s_3)^5 = 1\rangle.$$

We can now recognize these as Coxeter systems.

It is important to realize that a given group may possess several completely different Coxeter systems.

Example 1: Consider the dihedral group D_6. First of all, if we take the presentation

$$D_6 = \langle s_1, s_2 \mid (s_1)^2 = (s_2)^2 = (s_1 s_2)^6 = 1\rangle$$

from §1-3, then we have an irreducible Coxeter system of rank 2. On the other hand, we have the group decomposition

$$D_6 = D_3 \times \mathbb{Z}/2\mathbb{Z},$$

where the factors can be given the following Coxeter group structures

$$D_3 = \langle s_1, s_2 \mid (s_1)^2 = (s_2)^2 = (s_1 s_2)^3 = 1\rangle$$
$$\mathbb{Z}/2\mathbb{Z} = \langle s_3 \mid (s_3)^2 = 1\rangle.$$

So we can also impose a reducible Coxeter system of rank 3 on D_6.

Example 2: A similar type of pattern of a group possessing several different Coxeter systems holds for the automorphism group of the cube studied in §1-6. The two descriptions

$$(\mathbb{Z}/2\mathbb{Z})^3 \rtimes \Sigma_3 = \Sigma_4 \times \mathbb{Z}/2\mathbb{Z}$$

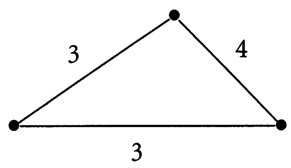
of the group given there can be used to obtain two completely different Coxeter systems. It has already been pointed out that $(\mathbb{Z}/2\mathbb{Z})^3 \rtimes \Sigma_3 = W(B_3)$, the reflection group associated to the root system B_3. The Coxeter system associated to this reflection group is irreducible and of rank 3. On the other hand, $\Sigma_4 = W(A_3)$ possesses a Coxeter system of rank 3, so $\Sigma_4 \times \mathbb{Z}/2\mathbb{Z}$ also has a reducible Coxeter system of rank 4.

Because of the existence of problems such as these, we shall deal with Coxeter systems rather than Coxeter groups. As our examples illustrate, the concepts of rank and reducibility are not well defined for Coxeter groups, only for Coxeter systems.

It is very convenient to represent Coxeter systems by graphs. Notably, throughout Chapter 8, we shall work with Coxeter graphs rather than Coxeter systems. A *Coxeter graph* is a graph with each edge labelled by an integer ≥ 3. There is a standard method of assigning a Coxeter graph to a Coxeter system. Given (W, S), let X be the graph where

(i) $S =$ the vertices of X;
(ii) given $s, s' \in S$ there is no edge between s and s' if $m_{ss'} = 2$;
(iii) given $s, s' \in S$ there is an edge labelled by $m_{s,s'}$ if $m_{ss'} \geq 3$.

This assignment sets up a one-to-one correspondence between Coxeter system and Coxeter graphs. For example, the Coxeter graph

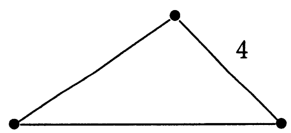


corresponds to the Coxeter presentation

$$W = \left\langle s_1, s_2, s_3 \;\middle|\; \begin{array}{c} (s_1s_2)^3 = (s_1s_3)^4 = (s_2s_3)^3 = 1 \\ (s_1)^2 = (s_2)^2 = (s_3)^2 = 1 \end{array} \right\rangle.$$

Coxeter graphs provide excellent models for Coxeter systems. Notice, in particular, that (W, S) *is irreducible if and only if its Coxeter graph X is connected.*

We also adopt one more convention. Because of the prevalence of $m_{ss'} = 3$, *we shall suppress the number* 3 *in our graphs.* So the above Coxeter graph now becomes



One goal of this chapter, as well as of the next two, is to set up a direct relation between finite Euclidean reflection groups and finite Coxeter systems. We shall define a map

$$\Psi\colon \left\{\begin{array}{c}\text{isomorphism classes of}\\ \text{finite reflection groups}\end{array}\right\} \to \left\{\begin{array}{c}\text{isomorphism classes of}\\ \text{finite Coxeter systems}\end{array}\right\}$$

and study its properties. The rest of Chapter 6 will be devoted to a discussion of this map, namely, how to associate a Coxeter system with a finite reflection subgroup. Actually, we shall deal with a refinement of the map where we use stable isomorphism classes of finite reflection groups. The map and this refinement will be introduced in the next section.

6-2 Reflection groups are Coxeter groups

In this section, we explain the basic procedure for associating Coxeter systems to finite Euclidean reflection groups. Given a finite reflection subgroup $W \subset O(\mathbb{E})$, we want to locate $S \subset W$ such that (W, S) is a Coxeter system, and such that the choice of S is unique up to isomorphism.

We choose S, as in §4-1. Think of W as the associated reflection group $W(\Delta)$ of an unitary root system Δ. Choose a fundamental system $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$ of Δ and let $S = \{s_{\alpha_i}\}$ be the corresponding fundamental reflections. Alternatively, S consists of the reflections in the walls of the chamber of Δ determined by Σ. By Proposition 4-1, S generates W. Given $1 \leq i, j \leq \ell$, let

$$m_{ij} = \text{the order of } s_{\alpha_i} s_{\alpha_j}.$$

In this section, we shall prove

***Theorem* (Coxeter)** $W(\Delta) = \langle \{s_{\alpha_i}\} \mid (s_{\alpha_i} s_{\alpha_j})^{m_{ij}} = 1 \rangle$.

Before proving the theorem, we shall make a few comments.

Remark 1: The associated Coxeter presentation $W = \langle \{s_{\alpha_i}\} \mid (s_{\alpha_i} s_{\alpha_j})^{m_{ij}} = 1 \rangle$ of a reflection group $W \subset O(\mathbb{E})$ arises from, and mirrors, precise facts about the geometry of W, namely the pattern or configuration formed by the hyperplanes of the reflections in W.

(i) The choice of generators $S \subset W$ is based on geometric data, since S consists of the set of reflections in the walls of the chamber determined by the fundamental system $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$. These walls are the hyperplanes $\{H_{\alpha_1}, \ldots, H_{\alpha_\ell}\}$.
(ii) The integers m_{ij} ($=$ order of $s_{\alpha_i} s_{\alpha_j}$) appearing in the Coxeter presentation also have a geometric content. By Lemma 1-4B, $\pi - \frac{\pi}{m_{ij}}$ is the angle between α_i and α_j. So they tell us about the angle at which the vectors $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$ meet each other. Since these vectors are orthogonal to the reflecting hyperplanes $\{H_{\alpha_1}, \ldots, H_{\alpha_\ell}\}$, this is information about the pattern formed by the hyperplanes of W.

Remark 2: The Coxeter presentation $\langle \{s_{\alpha_i}\} \mid (s_{\alpha_i} s_{\alpha_j})^{m_{ij}} = 1 \rangle$ given by the above theorem requires the choice of a fundamental system of Δ. However, up to isomorphism, the presentation is independent of such a choice. For, as shown in §4-6, W acts transitively on the fundamental systems. Given fundamental systems Σ and Σ', suppose $\varphi \cdot \Sigma = \Sigma'$. If S and S' are the sets of reflections corresponding to Σ and Σ', then, by property (A-4) of §1-1, the inner automorphism $\varphi\_\varphi^{-1}\colon W \to W$ sends S to S', thereby inducing an isomorphism between the presentations $W = \langle \{s_{\alpha_i}\} \mid (s_{\alpha_i} s_{\alpha_j})^{m_{ij}} = 1 \rangle$ and $W = \langle \{s'_{\alpha_i}\} \mid (s'_{\alpha_i} s'_{\alpha'_i})^{m'_{ij}} = 1 \rangle$.

Isomorphisms of reflection groups were defined in §1-1. We can easily extend the above remark to assert that any two isomorphic reflection groups determine the same isomorphism class of Coxeter systems. It follows that we have a well defined map

$$\Psi\colon \left\{ \begin{matrix} \text{isomorphism classes of} \\ \text{finite reflection groups} \end{matrix} \right\} \to \left\{ \begin{matrix} \text{isomorphism classes of} \\ \text{finite Coxeter systems} \end{matrix} \right\}.$$

We shall continue to study and refine the map Ψ, both in this chapter and in Chapter 8. We can make one immediate refinement. The concept of stable

isomorphism for reflection groups was introduced in §2-4. We can further extend Remark 2 to assert any two stably isomorphic reflection groups determine the same isomorphism class of Coxeter systems. So we actually have a well defined map

$$\Psi: \left\{\begin{matrix}\text{stable isomorphism classes}\\ \text{of finite reflection groups}\end{matrix}\right\} \to \left\{\begin{matrix}\text{isomorphism classes of}\\ \text{finite Coxeter systems}\end{matrix}\right\}.$$

It will be shown in §6-3 that this refined map is injective, and in Chapter 8 that it is surjective.

Proof of Theorem (Steinberg) $W(\Delta)$ is generated by $S = \{s_{\alpha_i}\}$. Any relation in $W(\Delta)$ is an equation between two monomials formed from the elements of S. If desired, any relation in $W(\Delta)$ can be put in the form

$$(*) \qquad s_{\beta_1} s_{\beta_2} \cdots s_{\beta_k} = 1$$

(i.e., all terms in the relation can be transferred to the LHS). Here each β_i is chosen from the fundamental roots $S = \{\alpha_i\}$ with repetitions being allowed. Moreover, any relation $(*)$ can be rewritten as

$$(**) \qquad \begin{gathered} s_{\beta_2} s_{\beta_3} \cdots s_{\beta_k} s_{\beta_1} = 1 \\ s_{\beta_3} s_{\beta_4} \cdots s_{\beta_k} s_{\beta_1} s_{\beta_2} = 1 \\ s_{\beta_4} s_{\beta_5} \cdots s_{\beta_m} s_{\beta_1} s_{\beta_2} s_{\beta_3} = 1, \\ \text{etc.} \end{gathered}$$

Now, suppose that there are relations that are not consequences of the given relations $(s_{\alpha_i} s_{\alpha_j})^{m_{ij}} = 1$. We shall assume that $(*)$ is such a relation. We shall also assume that our relation $(*)$ is chosen with k as small as possible. We want to show that these assumptions on $(*)$ produce a contradiction.

First of all, since $\det(s_{\beta_1} \cdots s_{\beta_k}) = (-1)^k$, we must have

$$k = 2m.$$

To produce a contradiction, it will suffice to show

$$(***) \qquad \begin{gathered} s_{\beta_1} = s_{\beta_3} = \cdots = s_{\beta_{2m-1}} \\ s_{\beta_2} = s_{\beta_4} = \cdots = s_{\beta_{2m}} \end{gathered}$$

because then relation $(*)$ becomes $(s_{\beta_1} s_{\beta_2})^m = 1$. But, since $m_{\beta_1 \beta_2}$ is the order of $s_{\beta_1} s_{\beta_2}$, we must have $m_{\beta_1 \beta_2} | m$. So $(*)$ is a consequence of the given relations $\{(s_{\alpha_i} s_{\alpha_j})^{m_{ij}} = 1\}$ and we have our contradiction.

The only part of $(***)$ we shall prove is $s_{\beta_1} = s_{\beta_3}$. To prove the remaining parts of $(***)$, we rewrite relation $(*)$ in the versions $(**)$ and apply the same argument. We shall prove $s_{\beta_1} = s_{\beta_3}$ by deducing the two relations

(I) $s_{\beta_1}s_{\beta_2}\cdots s_{\beta_m} = s_{\beta_2}s_{\beta_3}\cdots s_{\beta_{m+1}}$;
(II) $s_{\beta_3}s_{\beta_2}\cdots s_{\beta_m} = s_{\beta_2}s_{\beta_3}\cdots s_{\beta_{m+1}}$.

We can equate the LHS of (I) and (II) and cancel to obtain $s_{\beta_1} = s_{\beta_3}$.

Proof of Relation (I) Relation $(*)$ can be rewritten as

(i) $s_{\beta_1}s_{\beta_2}\cdots s_{\beta_{m+1}} = s_{\beta_{2m}}s_{\beta_{2m-1}}\cdots s_{\beta_{m+2}}$.

This equation shows that $\ell(s_{\beta_1}s_{\beta_2}\cdots s_{\beta_{m+1}}) < m+1$. By the Matsumoto Exchange Property of §4-4, there exists $1 \leq j \leq m$ so that

(ii) $s_{\beta_i}s_{\beta_{i+1}}\cdots s_{\beta_j} = s_{\beta_{i+1}}\cdots s_{\beta_{j+1}}$.

We are left with proving that $i = 1$, $j = m$. If not, then relation (ii) involves $< 2m = k$ terms and, so, is deducible from the given relations $\{(s_{\alpha_i}s_{\alpha_j})^{m_{ij}} = 1\}$. But then the relation

(iii) $s_{\beta_1}s_{\beta_2}\cdots s_{\beta_{2m}} = s_{\beta_1}\cdots \hat{s}_{\beta_i}\cdots \hat{s}_{\beta_{j+1}}\cdots s_{\beta_{2m}}$

(which is obtained by multiplying (ii) on the left by $s_{\beta_1}\cdots s_{\beta_{i-1}}$ and on the right by $s_{\beta_{j+1}}\cdots s_{\beta_{2m}}$) is also deducible from the given relations. Moreover, in view of relation $(*)$, we can equate the RHS of (iii) to 1. So we have

(iv) $s_{\beta_1}\cdots \hat{s}_{\beta_i}\cdots \hat{s}_{\beta_{j+1}}\cdots s_{\beta_{2m}} = 1$.

Since (iv) involves $< 2m = k$ terms, it is also deducible from the given relations. Combining (iii) and (iv), relation $(*)$ is deducible from the given relations, a contradiction.

Proof of Relation (II) We can rewrite relation $(*)$ as the relation $s_{\beta_2}\cdots s_{\beta_{2m}}s_{\beta\alpha_1} = 1$ and then argue, as in the proof of (I), to deduce

$$s_{\beta_2}\cdots s_{\beta_{m+1}} = s_{\beta_3}\cdots s_{\beta_{m+2}}.$$

We then rewrite this relation as

$$s_{\beta_3}(s_{\beta_2}\cdots s_{\beta_{m+1}})s_{\beta_{m+2}}s_{\beta_{m+1}}\cdots s_{\beta_4} = 1$$

and argue, as in the proof of (I), to obtain

$$s_{\beta_3}s_{\beta_2}\cdots s_{\beta_m} = s_{\beta_2}\cdots s_{\beta_{m+1}}.$$

■

Remark 3: The above theorem can be generalized. If we examine the above proof, we see that W being a Coxeter group was deduced from the fact that W is generated by a set of involutions satisfying the Matsumoto Exchange Property or, equivalently, the Matsumoto Cancellation Property. A reverse implication is also true. The more general result is that, given a group W generated by a set S of involutions, then (W, S) is a Coxeter system if and only if the set S satisfies the Matsumoto Exchange Property or the Matsumoto Cancellation Property.

6-3 The uniqueness of Coxeter structures

In this section, we want to demonstrate that, in many cases, the Coxeter presentation $W = \langle \{s_{\alpha_i}\} \mid (s_{\alpha_i}s_{\alpha_j})^{m_{ij}} = 1\rangle$ of a finite reflection group $W \subset O(\mathbb{E})$ is unique. In other words, it characterizes the reflection group up to stable isomorphism. Therefore, the map

$$\Psi : \left\{\begin{matrix}\text{stable isomorphism classes}\\ \text{of finite reflection groups}\end{matrix}\right\} \to \left\{\begin{matrix}\text{isomorphism classes of}\\ \text{finite Coxeter systems}\end{matrix}\right\}$$

introduced in §6-2 is injective. In Chapter 8 we shall show that Ψ is also surjective (see the discussion following Theorems 8-1A and 8-1B). We shall then have established a one-to-one correspondence between stable isomorphism classes of finite Euclidean reflection groups and isomorphism classes of finite Coxeter systems.

Our study will be centred on essential reflection groups. Such reflection groups were introduced in §2-4, and it was observed in §2-5 that every stable isomorphism class is uniquely represented by an essential reflection group. The following proposition demonstrates that if we limit our attention to such groups then their Coxeter presentations actually do give complete information.

Proposition *Two finite essential reflection groups are isomorphic if and only if their associated Coxeter systems are isomorphic.*

Consequently, the map Ψ is injective, as desired.

The rest of this section is devoted to the proof of the proposition. Throughout the proof *we shall assume that the root system Δ is unitary.* There are two properties of such root systems that will play a significant role in the proof. For any $\alpha, \beta \in \Delta$, we have

(C-1) $s_\alpha \cdot \beta = \beta - 2(\alpha, \beta)\alpha$

(C-2) $s_\alpha s_\beta$ has order $m \Leftrightarrow$ the angle between α and β is $\pi - \frac{\pi}{m}$

$$\Leftrightarrow (\alpha, \beta) = -\cos\left(\frac{\pi}{m}\right).$$

The formula in (C-1) is a simplification of that given in property (A-1) of §1-1. The simplification arises from the fact that we are dealing with an unitary root system. We have already observed, in Remark 1 of §6-2, that the first equivalence in (C-2) is true. As regards the second equivalence, the trigonometric identity $(\alpha, \beta) = \|\alpha\|\,\|\beta\|\cos\theta$, and the fact that we are dealing with unitary root systems, tell us

$$(\alpha, \beta) = \cos\left(\pi - \frac{\pi}{m}\right) = -\cos\left(\frac{\pi}{m}\right).$$

Proof of Proposition We have already demonstrated that isomorphic finite Euclidean reflection groups have isomorphic Coxeter systems. (See Remark 2 of §6-2.) Conversely, suppose we have essential reflection groups $W \subset O(\mathbb{E})$ and $W' \subset O(\mathbb{E}')$, and that their associated Coxeter systems (W, S) and (W', S') are isomorphic. In other words, we have a one-to-one correspondence between the

elements of $S = \{s_1, \ldots, s_\ell\}$ and $S' = \{s'_1, \ldots, s'_\ell\}$ so that $m_{ij} = m'_{ij}$, where m_{ij} (respectively m'_{ij}) is the order of $s_i s_j$ (respectively $s'_i s'_j$). We want to construct an isomorphism $f\colon \mathbb{E} \to \mathbb{E}'$ preserving inner products and conjugates W into W', i.e., $fWf^{-1} = W'$.

Let us recall how the Coxeter systems arise. Choose unitary root systems $\Delta \subset \mathbb{E}$ and $\Delta' \subset \mathbb{E}'$ of W and W'. The generators S and S' correspond to fundamental systems $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\} \subset \Delta$ and $\Sigma' = \{\alpha'_1, \ldots, \alpha'_\ell\} \subset \Delta'$ in the sense that, for each $1 \leq k \leq \ell$, we have

$$s_k = \text{the reflection } s_{\alpha_k}$$

$$s'_k = \text{the reflection } s_{\alpha'_k}.$$

The desired isomorphism between the reflection groups $W \subset O(\mathbb{E})$ and $W' \subset O(\mathbb{E}')$ is given by the linear transformation

$$f\colon \mathbb{E} \to \mathbb{E}'$$

$$f(\alpha_i) = \alpha'_i.$$

We need to verify two properties of f. First of all, f preserves inner products, i.e.,

$$\big(f(x), f(y)\big) = (x, y) \quad \text{for all } x, y \in \mathbb{E}.$$

By linearity, it suffices to show that this identity holds with x and y chosen from the basis $\{\alpha_1, \ldots, \alpha_\ell\}$. The fact that the associated Coxeter systems are the same (i.e., $m_{ij} = m'_{ij}$) forces

$$(\alpha_i, \alpha_j) = (\alpha'_i, \alpha'_j) \quad \text{for } 1 \leq i, j \leq \ell.$$

We use property (C-2) to deduce this.

Secondly, f conjugates W into W'. This follows from the next lemma.

Lemma *For each $1 \leq i \leq \ell$, we have $fs_{\alpha_i}f^{-1} = s_{\alpha'_i}$, i.e., we have a commutative diagram.*

$$\begin{array}{ccc} \mathbb{E} & \xrightarrow{f} & \mathbb{E}' \\ {\scriptstyle s_{\alpha_i}}\downarrow & & \downarrow{\scriptstyle s_{\alpha'_i}} \\ \mathbb{E} & \xrightarrow{f} & \mathbb{E}' \end{array}$$

Proof It suffices to show that the diagram commutes for the elements $\{\alpha_1, \ldots, \alpha_\ell\}$. We have already observed that $(\alpha_i, \alpha_j) = (\alpha'_i, \alpha'_j)$ for $1 \leq i, j \leq \ell$. We have

$$s_{\alpha'_i} f(\alpha_j) = s_{\alpha'_i} \cdot \alpha'_j = \alpha'_j - 2(\alpha'_i, \alpha'_j)\alpha'_i$$

$$\begin{aligned} fs_{\alpha_i}(\alpha_j) &= f[\alpha_j - 2(\alpha_i, \alpha_j)\alpha_i] = f(\alpha_j) - 2(\alpha_i, \alpha_j)f(\alpha_i) \\ &= \alpha'_j - 2(\alpha'_i, \alpha'_j)\alpha'_i. \end{aligned}$$

■

It follows from the lemma that the isomorphism

$$\widetilde{f}\colon O(\mathbb{E}) \to O(\mathbb{E}')$$
$$\varphi \to f\varphi f^{-1}$$

sends W to W'. First of all, W is mapped into W' because $\{s_{\alpha_1}, \ldots, s_{\alpha_\ell}\}$ generate W and they are sent by $\widetilde{f}$ into W'. Secondly, W is mapped onto W' because $\{s'_{\alpha_1}, \ldots, s'_{\alpha_\ell}\}$ generate W', and they belong to $\operatorname{Im} \widetilde{f}$.

7 Bilinear forms of Coxeter systems

In this chapter, we associate a canonical bilinear form to a finite Coxeter system and study its properties. The construction is motivated by the relation between finite reflection groups and Coxeter systems developed in §6-2. The main result of this chapter is that the bilinear form associated to a Coxeter system is always positive definite. In Chapter 8, we shall use the positive definiteness of this bilinear form to classify both finite Coxeter systems and finite Euclidean reflection groups.

7-1 The bilinear form of a Coxeter system

Appendix B contains a brief treatment of bilinear forms, including basic definitions. We want to associate a bilinear form to every finite Coxeter system. The definition we give is motivated by the situation for reflection groups. Let us recall some basic facts from Chapter 6. Let $W \subset O(\mathbb{E})$ be a finite Euclidean reflection group with unitary root system Δ. Let

$$\Sigma = \{\alpha_1, \ldots, \alpha_\ell\} \subset \Delta$$

be a fundamental system and let

$$S = \{s_{\alpha_1}, \ldots, s_{\alpha_\ell}\}$$

be the fundamental reflections corresponding to $\{\alpha_1, \ldots, \alpha_\ell\}$. Then (W, S) is a Coxeter system. It was observed in property (C-2) of §6-3 that the inner product on $\mathbb{E}$ satisfies

$$(\alpha_i, \alpha_j) = -\cos\left(\frac{\pi}{m_{ij}}\right) \Leftrightarrow s_{\alpha_i}s_{\alpha_j} \text{ has order } m_{ij}.$$

This relation suggests a way of defining a bilinear form for a finite Coxeter system (W, S). Let

$$\mathbb{V} = \text{a vector space over } \mathbb{R} \text{ with basis } \{e_s \mid s \in S\}.$$

Define a bilinear form $\mathcal{B}\colon \mathbb{V} \times \mathbb{V} \to \mathbb{R}$ by

$$\mathcal{B}(e_s, e_{s'}) = -\cos\left(\frac{\pi}{m_{ss'}}\right).$$

In particular, $\mathcal{B}(e_s, e_s) = 1$ while $\mathcal{B}(e_s, e_{s'}) = 0$ when $m_{ss'} = 2$.

If $\mathbb{E}$ is a Euclidean space, $W \subset O(\mathbb{E})$ is a reflection group, and (W, S) is the associated Coxeter system, then $\mathcal{B}$ can be identified with the original inner product on $\mathbb{E}$. (Identify the basis elements $\{e_1, \ldots, e_\ell\}$ with the fundamental roots $\{\alpha_1, \ldots, \alpha_\ell\}$.) So, in the case of finite reflection groups, $\mathcal{B}$ must be positive definite. This chapter will be devoted to proving that this positive definiteness result actually holds for all finite Coxeter groups. In this chapter we shall prove:

Theorem *The bilinear form $\mathcal{B}$ is positive definite for every finite Coxeter system (W, S).*

Remark: This theorem has various generalizations. Although we are only discussing the finite case, we can actually define the bilinear form for any Coxeter system (when $m_{ss'} = \infty$, we let $\mathcal{B}\big((e_s, e_{s'})\big) = -1$). In this context, the converse of the theorem is also true. Namely, the bilinear form $\mathcal{B}$ is positive definite if and only if W is finite. Characterization of Coxeter systems using their associated bilinear forms holds in another case as well. The affine Weyl groups to be considered in Chapter 11 have canonical Coxeter system characterized by their associated bilinear form being nonnegative, i.e., $\mathcal{B}(x,x) \geq 0$ for all $x \in \mathbb{V}$.

In §7-2 we shall prove some preliminary results, in particular that there is a well defined canonical action of W on $\mathbb{V}$ for which the form $\mathcal{B}$ is W*-invariant*, i.e.,

$$\mathcal{B}(\varphi \cdot x, \varphi \cdot y) = \mathcal{B}(x,y) \text{ for all } x, y \in \mathbb{V} \text{ and } \varphi \in W.$$

In §7-3 we shall prove that $\mathcal{B}$ is positive definite.

At the moment, we want to observe that, for any (W,S), $\mathcal{B}$ is always positive definite on certain subspaces of $\mathbb{V}$. Given $s, s' \in S$ let

$$\mathbb{V}_{s,s'} = \mathbb{R}e_s + \mathbb{R}e_{s'}.$$

Lemma *For any $s, s' \in S$, the restriction of $\mathcal{B}$ to $\mathbb{V}_{s,s'}$ is positive definite.*

Proof Choose an arbitrary $x = ae_s + be_{s'} \in \mathbb{V}_{s,s'}$. Let $m = m_{ss'}$. Then

$$\begin{aligned}\mathcal{B}(x,x) &= \mathcal{B}(ae_s + be_{s'}, ae_s + be_{s'}) = a^2 + b^2 - 2ab\cos\left(\frac{\pi}{m}\right)\\ &= a^2 - 2ab\cos\left(\frac{\pi}{m}\right) + b^2\cos^2\left(\frac{\pi}{m}\right) + b^2\sin^2\left(\frac{\pi}{m}\right)\\ &= \left[a - b\cos\left(\frac{\pi}{m}\right)\right]^2 + \left[b\sin\left(\frac{\pi}{m}\right)\right]^2. \qquad \blacksquare\end{aligned}$$

As a final observation, we can pass from Coxeter systems to Coxeter graphs and just as easily define the associated bilinear form $\mathcal{B} = \mathcal{B}_X$ for a Coxeter graph X. It is defined exactly as above. The information required to define the bilinear form is present in the graph. The vertices come from the set $S = \{s\}$, while the integers $\{m_{ss'}\}$ are the labels of the edges. (Recall that $m = 3$ is suppressed.) Throughout Chapter 8, we shall be working with Coxeter graphs rather than Coxeter systems.

7-2 The Tits representation

Let (W,S) be a finite Coxeter system and let $\mathcal{B}\colon \mathbb{V} \times \mathbb{V} \to \mathbb{R}$ be the associated bilinear form as defined in §7-1. In this section, we shall define an action of W on $\mathbb{V}$. This action is of interest in its own right; for it defines a "reflection representation" $\rho\colon W \to O(\mathbb{V})$, where

$$O(\mathbb{V}) = \{f\colon \mathbb{V} \to \mathbb{V} \text{ linear isomorphism where } \mathcal{B}\big(f(x), f(y)\big) = \mathcal{B}(x,y)\}$$

is the orthogonal group of $\mathcal{B}$. We are defining the action, however, because it will be needed in §7-3 during the proof that $\mathcal{B}$ is positive definite.

As with the bilinear form, the W action on $\mathbb{V}$ is motivated by the relation developed in §6-2 between finite reflection groups and finite Coxeter systems. It was observed in property (C-1) of §6-3 that the fundamental reflections $\{s_{\alpha_1}, \ldots, s_{\alpha_\ell}\}$ and the fundamental roots $\{\alpha_1, \ldots, \alpha_\ell\}$ are related by the rule:

$$s_{\alpha_i} \cdot \alpha_j = \alpha_j - (\alpha_i, \alpha_j)\alpha_i.$$

This suggests how to define a representation $\rho\colon W \to O(\mathbb{V})$ for (W, S). We shall use the notation from §7-1. For each $s \in S$, define the linear transformation $\rho(s)\colon \mathbb{V} \to \mathbb{V}$ by

$$\rho(s)(x) = x - 2\mathcal{B}(x, e_s)e_s.$$

We can show that this definition works out, and that we have a well defined map $\rho\colon W \to O(\mathbb{V})$. Even more is true. The map ρ is always injective and, in the finite case, $W \subset O(\mathbb{V})$ is a reflection group with the set S being fundamental reflections. However, fairly involved arguments are needed to establish these latter results. As we have already said, we are focusing on the more restricted result that the bilinear form $\mathcal{B}$ is positive definite in the finite case. To establish this result, we only need to construct a well defined homomorphism $\rho\colon W \to O(\mathbb{V})$. In the rest of this section, we shall show that the map $\rho\colon S \to O(\mathbb{V})$ extends to a group homomorphism

$$\rho\colon W \to O(\mathbb{V}).$$

Recall that $W = F/N$ where

$$F = \text{the free group generated by } S$$

$$R = \{(ss')^{m_{ss'}} \mid s, s' \in S\}$$

$$N = \bigcap_{R \subset K \lhd F} K\,.$$

We certainly can extend $\rho\colon S \to O(\mathbb{V})$ to a group homomorphism

$$\rho\colon F \to O(\mathbb{V}).$$

To prove ρ factors through $W = F/N$, it suffices to show:

Proposition *For each $s, s' \in S$, $\rho(s)\rho(s')$ has order $m_{ss'}$.*

This proposition implies that $R \subset \operatorname{Ker}\rho$. Since $\operatorname{Ker}\rho \lhd F$, we then have $N \subset \operatorname{Ker}\rho$.

Proof of Proposition It follows from the definition of $\rho(s)$ that $\rho(s)^2 = 1$. So we can assume $s \neq s'$. Let

$$\mathbb{V}_{s,s'} = \mathbb{R}e_s + \mathbb{R}e_{s'}$$

$$\mathbb{V}_{s,s'}^{\perp} = \{x \in \mathbb{V} \mid \mathcal{B}(x, y) = 0 \text{ for all } y \in \mathbb{V}_{s,s'}\}.$$

Then $\mathbb{V} = \mathbb{V}_{s,s'} + \mathbb{V}_{s,s'}^{\perp}$. Since $\rho(s)\rho(s')$ maps $\mathbb{V}_{s,s'}$ to itself and leaves $\mathbb{V}_{s,s'}^{\perp}$ pointwise invariant, it follows that the order of $\rho(s)\rho(s')$ = the order of $\rho(s)\rho(s')|_{\mathbb{V}_{s,s'}}$. By Lemma 7-1, $\mathbb{V}_{s,s'}$ is the Euclidean plane. Since $\mathcal{B}(e_s, e_{s'}) = -\cos(\frac{\pi}{m_{ss'}})$, it follows as in property (C-2) of §6-3, that $\rho(s)\rho(s')|_{\mathbb{V}_{s,s'}}$ has order $m_{ss'}$. ■

As a final fact about the representation ρ, the construction has the important property of sending reducible Coxeter systems to reducible representations. Given a decomposition $(W,S) = (W_1,S_1) \times (W_2,S_2)$ of Coxeter systems, then $\rho \cong \rho_1 \oplus \rho_2$, where ρ, ρ_1 and ρ_2 are the representations associated to (W,S), (W_1,S_1) and (W_2,S_2), respectively. This follows from the definitions, and the fact that $m_{ss'} = 2$ whenever $s \in S_1$ and $s' \in S_2$.

7-3 Positive definiteness

In this section, we prove Theorem 7-1, namely that the associated bilinear form of a finite Coxeter system is positive definite. Throughout this section, we shall assume (W,S) *is a finite irreducible Coxeter system.* We shall denote the elements of S as $S = \{s_1, \ldots, s_\ell\}$, and let m_{ij} = the order of $s_i s_j$. Let $\mathcal{B}\colon \mathbb{V} \times \mathbb{V} \to \mathbb{R}$ be the associated bilinear form defined in §7-1. Let $\rho\colon W \to O(\mathbb{V})$ be the representation (i.e., the action of W on $\mathbb{V}$) defined in §7-2. Let $\{e_1, \ldots, e_\ell\}$ be the basis of $\mathbb{V}$ satisfying

$$\mathcal{B}(e_i, e_j) = \cos\left(\frac{\pi}{m_{ij}}\right)$$

$$\rho(s_i) \cdot x = x - \mathcal{B}(x, e_i)e_i.$$

In proving that $\mathcal{B}$ is positive definite for finite Coxeter systems, it is reasonable to make the above assumption of irreducibility. For, if $(W,S) = (W_1,S_1) \times (W_2,S_2)$, then $\mathcal{B} \cong \mathcal{B}_1 \oplus \mathcal{B}_2$, where $\mathcal{B}$, $\mathcal{B}_1$ and $\mathcal{B}_2$ are the bilinear forms constructed from (W,S), (W_1,S_1) and (W_2,S_2). So if $\mathcal{B}_1$ and $\mathcal{B}_2$ are positive definite, then B is too.

Definition: $\mathbb{V}^{\perp} = \{x \in \mathbb{V} \mid \mathcal{B}(x,y) = 0 \text{ for all } y \in \mathbb{V}\}$.

We begin by showing that $\mathbb{V}^{\perp} = 0$, i.e., $\mathcal{B}$ is nondegenerate. This result will be a corollary of the next proposition. Observe that $\mathcal{B} \neq 0$ implies $\mathbb{V}^{\perp} \neq \mathbb{V}$. Also, $\mathbb{V}^{\perp}$ is invariant under W. For, consider $x \in \mathbb{V}^{\perp}$. If we suppress the symbol ρ, then, for all $y \in \mathbb{V}$ and $\varphi \in W$, we have the identities

$$\mathcal{B}(\varphi \cdot x, y) = \mathcal{B}(x, \varphi^{-1} \cdot y) = 0.$$

The first identity follows from the W-invariance of $\mathcal{B}$.

Proposition A *If $0 \neq U \subset \mathbb{V}$ is a proper subspace preserved under the action of W, then $U \subset \mathbb{V}^{\perp}$.*

Proof The irreducibility of the Coxeter system (W,S) implies that

$$(*) \qquad e_i \notin U \quad \text{for all } 1 \leq i \leq \ell.$$

To see this, partition $S = S_1 \coprod S_2$, where

$$S_1 = \{s_i \mid e_i \in U\} \quad \text{and} \quad S_2 = \{s_j \mid e_j \notin U\}.$$

Since U is proper, we know $S_2 \neq \varnothing$. Suppose $S_1 \neq \varnothing$.

(i) By the irreducibility of (W, S) there exists $s_i \in S_1$ and $s_j \in S_2$ such that $\mathcal{B}(e_i, e_j) \neq 0$. Otherwise, the elements of S_1 and S_2 commute with each other and, so, there exists a decomposition $(W, S) = (W_1, S_1) \times (W_2, S_2)$.

(ii) On the other hand, since U is mapped to itself under the action of W, $e_i \in U$ means that $\rho(s_j) \cdot e_i \in U$ as well. Thus $2\mathcal{B}(e_i, e_j)e_j = e_i - \rho(s_j) \cdot e_i \in U$. Since $e_j \notin U$, this means $\mathcal{B}(e_i, e_j) = 0$.

The contradiction produced by (i) and (ii) demonstrates that we must have $S_1 = \varnothing$, which establishes $(*)$.

Now choose $x \in U$. We can use $(*)$ to prove $x \in \mathbb{V}^{\perp}$. We want to prove $\mathcal{B}(x, e_i) = 0$ for all $1 \leq i \leq \ell$. Pick e_i. As above, $2\mathcal{B}(x, e_i)e_i = x - \rho(s_i) \cdot x \in U$. However, by $(*)$, $e_i \notin U$. Thus $\mathcal{B}(x, e_i) = 0$. ■

We can use Proposition A to deduce significant results about ρ and $\mathcal{B}$. Since we are working in characteristic 0, $\mathbb{V}$ is completely reducible as a W module (see Appendix B). On the other hand, Proposition A says that, given a nontrivial decomposition $\mathbb{V} = U \oplus U'$ of W modules, then both U and U' lie in $\mathbb{V}^{\perp}$. Since $\mathbb{V}^{\perp} \neq \mathbb{V}$, such nontrivial decompositions cannot exist. Thus we have:

Corollary A *The representation $\rho\colon W \to O(\mathbb{V})$ is irreducible.*

In particular, since $\mathbb{V}^{\perp} \neq \mathbb{V}$ and $\mathbb{V}^{\perp}$ is preserved under the action of W, we must have $\mathbb{V}^{\perp} = 0$. In other words:

Corollary B *$\mathcal{B}$ is nondegenerate.*

The fact that $\mathcal{B}$ is actually positive definite follows from the next proposition. Despite the lack of a designated inner product on $\mathbb{V}$, we can still talk about reflections acting on $\mathbb{V}$. By a *reflection*, we mean a linear transformation $s\colon \mathbb{V} \to \mathbb{V}$ that leaves a hyperplane $H \subset \mathbb{V}$ pointwise fixed and acts as multiplication by -1 on a complementary line L. It follows from Proposition D of Appendix C that:

Proposition B *Let $\rho\colon G \to O(\mathbb{V})$ be an irreducible representation of a finite group. Suppose an element of G acts on $\mathbb{V}$ (via ρ) as a reflection. Then any two G-invariant nondegenerate bilinear forms on $\mathbb{V}$ are multiples of each other.*

If we apply Proposition B to our particular representation $\rho\colon W \to O(\mathbb{V})$, we can deduce:

Corollary C *$\mathcal{B}$ is positive definite.*

Proof First of all, $\mathbb{V}$ has a W-invariant bilinear form that is positive definite. Just take any positive definite form $\mathcal{B}'$ and average it to obtain

$$\hat{\mathcal{B}}(x, y) = \frac{1}{|W|} \sum_{\varphi \in W} \mathcal{B}'(\varphi \cdot x, \varphi \cdot y).$$

Secondly, since $\mathcal{B}$ is nondegenerate and W-invariant, it follows from Proposition B that $\mathcal{B} = k\hat{\mathcal{B}}$. Thirdly, since $\mathcal{B}(e_i, e_i) = 1$, we must have $k > 0$. ∎

8 Classification of Coxeter systems and reflection groups

In this chapter, we obtain a classification of finite Coxeter systems and finite Euclidean reflection groups. We have already shown in Chapter 6 that every reflection group has a canonical associated Coxeter system. So the classifications are related. In Chapter 7 we introduced the bilinear form of a Coxeter system. Most of this chapter is occupied with determining necessary conditions for the bilinear form $\mathcal{B}\colon \mathbb{V} \times \mathbb{V} \to \mathbb{R}$ of a finite Coxeter system (W, S) to be positive definite. We then have strong restrictions on the possibilities for finite Coxeter systems. The classification is finished by proving that each of these remaining possibilities can be realized by the case of a finite reflection group.

8-1 Classification results

In this section, we describe the classification results for finite reflection groups and finite Coxeter systems that will be obtained in this chapter. In dealing with Coxeter systems, we shall use the Coxeter graph notation introduced in §6-1. Most of this chapter will be devoted to proving:

Theorem A *If (W, S) is a finite irreducible Coxeter system, then its Coxeter graph is one of the following:*

(A_ℓ) $(\ell \geq 1)$

$(B_\ell \text{ or } C_\ell)$ $(\ell \geq 2)$

(D_ℓ) $(\ell \geq 4)$

(E_6)

(E_7)

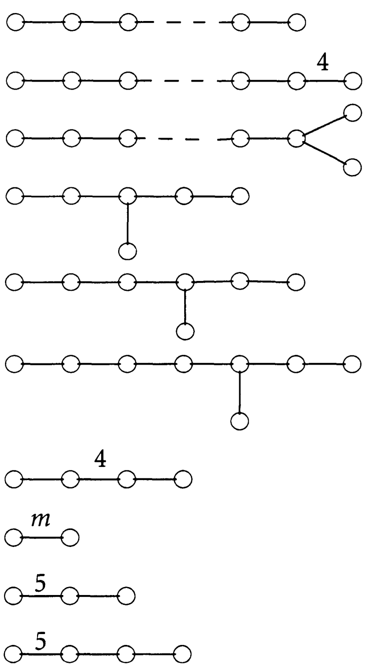
(E_8)

(F_4)

$(G_2(m))$

(H_3)

(H_4)



Remark 1: We have followed the traditional notation for Coxeter groups, with

one exception. The case we have labelled $G_2(m)$ for $m \geq 5$ is traditionally denoted by G_2 for $m = 6$ and by $I_2(m)$ for $m = 5$ or $m \geq 7$. The labelling for Coxeter groups originates from (and extends) that used for Weyl groups (see Chapter 10). In particular, this explains the double label given to the case $B_\ell = C_\ell$. It will bifurcate into the separate cases B_ℓ and C_ℓ when we turn to Weyl groups, i.e., when we work over $\mathbb{Z}$, rather than over $\mathbb{R}$.

We can complete the classification of finite Coxeter systems and finite Euclidean reflection groups by showing:

Theorem B *Each of the Coxeter systems represented by the Coxeter graphs A_ℓ, B_ℓ, $\ldots$, H_4 arises from a finite reflection group.*

It follows from Theorems A and B that the injective map

$$\Psi\colon \left\{\begin{matrix}\text{stable isomorphism classes}\\ \text{of finite reflection groups}\end{matrix}\right\} \to \left\{\begin{matrix}\text{isomorphism classes of}\\ \text{finite Coxeter systems}\end{matrix}\right\}$$

discussed in §6-2 and §6-3 is surjective and, hence, a one-to-one correspondence. Moreover, the isomorphism classes of the irreducible cases are then represented by the graphs in Theorem A. So we have a classification result.

Most of this chapter, namely §8-2, §8-3, §8-4 and §8-5, will be devoted to the proof of Theorem A. Theorem B will be dealt with in §8-6. If (W, S) is a finite Coxeter system and $\mathcal{B}\colon \mathbb{V} \times \mathbb{V} \to \mathbb{R}$ is its associated bilinear form, as defined in §7-1, then we know that the quadratic form

$$q(x) = \mathcal{B}(x, x)$$

must be positive definite. We shall prove Theorem A by studying this quadratic form and determining necessary conditions for it to be positive definite.

It is far more convenient to work with Coxeter graphs, rather than Coxeter systems. We already observed at the end of §7-1 that the bilinear form $\mathcal{B}\colon \mathbb{V}\times\mathbb{V} \to \mathbb{R}$ can just as easily be defined from a Coxeter graph as from a Coxeter system. And it will quickly become clear that it is much easier to formulate (and understand) the restrictions arising from $\mathcal{B}$ being positive definite in terms of Coxeter graphs, rather than in terms of Coxeter systems.

Remark 2: Several variations on the proof given in this chapter are possible.

(i) First of all, a more conceptual approach to the correspondence between reflection groups and Coxeter systems is possible. The proof given in this chapter is essentially a counting argument. We restrict the possibilities for finite Coxeter systems, and then produce a finite reflection group realizing each case left on the list. The more conceptual approach is based on the Tits representation defined in §7-2. We can use it to define the inverse of the map Ψ. However, this approach requires a great deal more machinery.

(ii) Secondly, if we are only interested in the classification of finite reflection groups, then a simpler argument than that used in this book is possible.

Namely, it is possible to ignore the results of Chapter 7. For, given an Euclidean reflection group $W \subset O(\mathbb{E})$, then the bilinear form of its associated Coxeter system is defined so as to agree with the originally given inner product on $\mathbb{E}$. Thus it is automatically positive definite. There is no need to justify this fact. We can now apply the arguments in this chapter to establish that the Coxeter systems of reflection groups satisfy the restrictions of Theorem A. In conjunction with Theorem B, we obtain a classification of finite essential reflection groups.

8-2 Preliminary results

In the next four sections, we shall study the associated bilinear form $\mathcal{B} = \mathcal{B}_X$ of a Coxeter graph X and obtain restrictions on when the quadratic form $q(x) = \mathcal{B}(x, x)$ is positive definite. The graph X will have vertices $S = \{s_1, \ldots, s_\ell\}$ and the edges will be labelled by the integers

$$m_{ij} = m_{s_i s_j}.$$

The vector space $\mathbb{V}$ will have basis $(e_1, \ldots, e_\ell)$ and the bilinear form $\mathcal{B}\colon \mathbb{V}\times\mathbb{V} \to \mathbb{R}$ is determined by the quantities

$$q_{ij} = \mathcal{B}(e_i, e_j) = -\cos\left(\frac{\pi}{m_{ij}}\right).$$

For, we have $\mathcal{B}(x, y) = \sum_{i,j} q_{ij} x_i y_j$. We shall assume that $\mathcal{B}$ is positive definite and deduce the consequences.

First of all, since we want to study irreducible Coxeter systems, we can assume that the *Coxeter graph X is connected.* A *tree* is a connected graph with no circuits.

Lemma A *X is a tree.*

Proof Suppose X contains a circuit $(s_{i_1}, \ldots, s_{i_k})$ where $k \geq 3$. Consider the element $x = e_{i_1} + \cdots + e_{i_k} \in \mathbb{V}$. We shall show that $q(x) \leq 0$ contradicting the positive definiteness of q. Since $q_{ii} = 1$ and $q_{ij} = q_{ji}$, we have

$$(*) \qquad q(x) = k + 2\sum q_{ij}.$$

The integers $m_{12}, \ldots, m_{k-1,k}, m_{k,1}$ are all ≥ 3. (This is equivalent to the existence of edges between s_{i_1} and s_{i_2}, s_{i_2} and s_{i_3}, etc.) Consequently, the definition $q_{ij} = \mathcal{B}(e_i, e_j) = -\cos(\frac{\pi}{m_{ij}})$ forces:

$(**)$ The numbers $q_{1,2}, \ldots, q_{k-1,k}, q_{k,1}$ are all $\leq -1/2$.

Combining $(*)$ and $(**)$, we have $q(x) \leq k - k = 0$. ■

We next use trigonometry to obtain an important restriction. Fix $1 \leq i \leq \ell$.

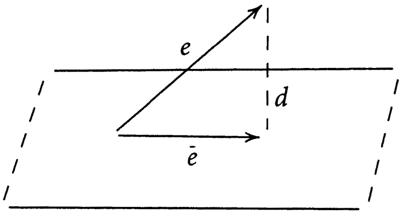
Lemma B $\sum_{j \neq i} q_{ij}^2 < 1$.

Proof In all that follows, i is fixed. Consider the set $J = (1 \le j \le \ell \mid j \ne i$ and $q_{ij} \ne 0)$. We claim that

$$(*) \qquad \{e_j\}_{j \in J} \text{ is an orthonormal basis of } U = \bigoplus_{j \in J} \mathbb{R} e_j.$$

Since $q_{jj} = 1$, it suffices to show $q_{jk} = 0$ for all $j \ne k \in J$. Now, $q_{jk} \ne 0$ means that there is an edge between s_j and s_k in the graph X. Since $q_{ij} \ne 0$ and $q_{ik} \ne 0$, there also are edges between s_i and s_j, as well as between s_i and s_k. The resulting circuit contradicts Lemma A.

Let d = distance of e_i to U. In the following picture, the dashed line is a perpendicular of d dropped from the top of e_i to U. We have also indicated $\bar{e}_i$, the projection of e_i onto U.



We have the resolution into orthogonal components

$$(**) \qquad \bar{e}_i = \sum_{j \in J} q_{ij} e_j = \sum_{j \ne i} q_{ij} e_j.$$

The first identity follows from $(*)$. The second identity is based on the fact that $q_{ij} = 0$ if $j \ne i$ and $j \notin J$.

It follows from the right-angled triangle in our picture that

$$||e_i||^2 = d^2 + ||\bar{e}_i||^2.$$

Substituting $(**)$ into the equation, we obtain

$$1 = d^2 + \sum_{j \ne i} (q_{ij})^2. \qquad \blacksquare$$

We can use Lemma B to obtain a series of important restrictions on the graph X.

Lemma C

(i) A vertex belongs to at most 3 edges.
(ii) A vertex belongs to 3 edges only if the edges are all of order 3.
(iii) A vertex belongs to at most one edge of order ≥ 4.
(iv) There exists an edge of order ≥ 6 *only if* X *has 2 vertices.*

Proof For all the restrictions, we use the inequality $(q_{ij})^2 < 1$ of Lemma B, and precise facts about the values of q_{ij}.

Case (i): The existence of an edge between s_i and s_j forces $(q_{ij})^2 \geq 1/4$ because $q_{ij} = -\cos(\frac{\pi}{m_{ij}})$, while the existence of the edge forces $m_{ij} \geq 3$.

Cases (ii), (iii) and (iv): We use the equivalences

$$m_{ij} = 3 \Leftrightarrow q_{ij} = -1/2$$
$$m_{ij} = 4 \Leftrightarrow q_{ij} = -1/\sqrt{2}$$
$$m_{ij} = 6 \Leftrightarrow q_{ij} = -\sqrt{3}/2. \qquad \blacksquare$$

8-3 The two possible cases

We know that X is a tree. A vertex is a *ramification point* if it belongs to more than two edges. A *chain* is a tree with no ramification points. In this section, we make use of a reduction argument to prove:

Proposition *There are only two possibilities for X:*

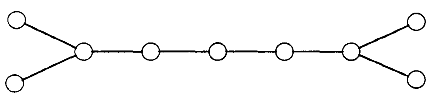
(i) X possesses a unique ramification point and all edges are of order 3;
(ii) X is a chain and at most one edge is of order ≥ 4.

In §8-4 and §8-5 we shall explore the ramification case and the chain case separately, and further reduce X to the possibilities given in Theorem 8-1A. We can prove the above proposition by showing that:

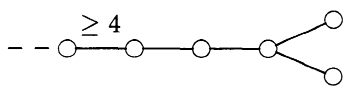
Reduction Result If X is a Coxeter graph such that the associated bilinear form is positive definite, then we can collapse any edge of order 3 (i.e., remove the edge and identify its two vertices) and the resulting Coxeter graph X' will also have an associated bilinear form that is positive definite.

For if such a reduction result is true, then we can prove the proposition by using Lemma 8-2C. Namely, if X does not satisfy (i) or (ii), then it must contain within itself one of the following three possibilities:

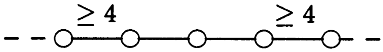
(a) two ramification points separated by edges of order 3



(b) a ramification point and an edge of order ≥ 4 separated by edges of order 3



(c) two edges of order ≥ 4 separated by edges of order 3.



In each case, if we use the reduction result (iteratively) to collapse the edges of order 3, the resulting graphs contradict Lemma 8-2C. Hence none of the above possibilities can occur.

Proof of the Reduction Result We are left to verify the reduction result. Let X be a Coxeter graph and let $I = (1, 2, \ldots, \ell)$ be the index set of the vertices $(s_1, \ldots, s_\ell)$ of X. Suppose s_k and s_n are vertices such that $m_{kn} = 3$.

Let X' be the Coxeter graph obtained from X by identifying s_k and s_n. Such an identification is allowable. There is an obvious problem to consider. Given a third vertex s_i, suppose there are edges of different orders running from s_i to s_k and s_n, respectively. Then, when we identify s_k and s_n, it is not clear how to assign an order to the edge running from s_i to this new vertex. However, such problems do not arise because $m_{kn} = 3$ means that there is an edge between s_k and s_n. If the other two edges existed, then there would be a circuit, contradicting Lemma 8-2A.

We shall let $I' = [I - \{k, n\}] \cup \{\rho\}$ be the index set for the vertices of X'. Here ρ indexes the new vertex obtained by identifying s_k and s_n. We want to compare the associated quadratic forms

$$q \colon \mathbb{V} \to \mathbb{R} \qquad q(x) = \sum_{i,j} q_{ij} x_i x_j$$

$$q' \colon \mathbb{V}' \to \mathbb{R} \qquad q'(x) = \sum_{i,j} q'_{ij} x'_i x'_j$$

of X and X'. We have $\dim \mathbb{V}' = \dim \mathbb{V} - 1$. We shall show that there is a canonical imbedding $\mathbb{V}' \subset \mathbb{V}$ so that $q' = q|_{\mathbb{V}'}$. Thus q positive definite forces q' positive definite. This, of course, is what we want to show.

Imbed $\mathbb{V}' \subset \mathbb{V}$ by the rule

$$\mathbb{V}' = \text{the subspace } \{x_k = x_n\}.$$

In other words, let

$$x_i = x'_i \quad \text{if } i \neq k, n$$
$$x_k = x'_\rho$$
$$x_n = x'_\rho.$$

Substituting these values in $q(x)$ we obtain

$$
\begin{aligned}
q|_{V'} &= \sum_{i,j\in I-\{k,n\}} q_{ij}x_i'x_j' + 2\sum_{i\neq k,n}(q_{ik}+q_{in})x_i'x_\rho' + 2q_{kn}(x_\rho')^2 + 2(x_\rho')^2 \\
(*) \qquad &= \sum_{i,j} q_{ij}'x_i'x_j' + (2q_{kn}+1)(x_\rho')^2 \\
&= q'(x) + (2q_{kn}+1)(x_\rho')^2.
\end{aligned}
$$

The second identity of $(*)$ is based on the fact that

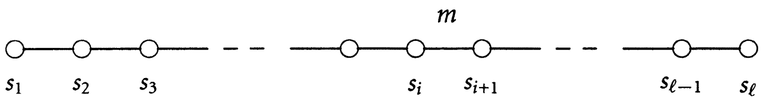
$$
\begin{aligned}
q_{ij}' &= q_{ij} \quad \text{if } i,j \in I-\{k,n\} \\
q_{i\rho}' &= q_{ik}+q_{in} \quad \text{if } i \in I-\{k,n\}.
\end{aligned}
$$

Here we are using the already-discussed fact that there cannot be edges in X from s_i to both s_k and s_n. So either $m_{ik}=2$, or $m_{in}=2$. Thus either $q_{ik}=0$, or $q_{in}=0$.

Finally, we can eliminate the term $(2q_{kn}+1)(x_\rho')^2$ from $(*)$ because $m_{kn}=3$ implies $q_{kn}=-1/2$. So equation $(*)$ becomes the desired $q_{|E'}=q'$.

8-4 The chain case

In this section, we further explore case (ii) of Proposition 8-3. We want to consider graphs of the form



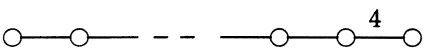
If $\ell=2$, then there are no restrictions on m. For, given $m\geq 3$, the graph $0\overset{m}{—}0$ is that of the dihedral group D_m. It is only for $\ell\geq 3$ that further restrictions on the graph X are possible. In that case, it follows from part (iv) of Lemma 8-2C that only $m\leq 5$ is allowable. So we must consider $m=3,4,5$. In this section, we prove:

Proposition *Given $\ell\geq 3$ and $3\leq m\leq 5$, then X is one of the following:*

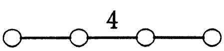
(i) $m=3$

 (A_ℓ)

(ii) $m=4$

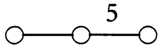


(B_ℓ)

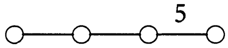


(F_4)

(iii) $m = 5$



(H_3)



(H_4)

Before proving the proposition, we first prove:

Length Lemma *Let $s_1, \ldots, s_k$ be vertices of X such that $(s_1 s_2), (s_2 s_3), \ldots, (s_{k-1} s_k)$ are edges of order 3. Let $v = e_1 + 2e_2 + \cdots + ke_k$. Then $\|v\|^2 = \frac{1}{2}k(k+1)$.*

Proof We have

$$(e_i, e_i) = 1$$

$$(e_i, e_{i+1}) = -\frac{1}{2}$$

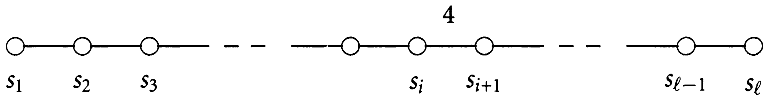
$$(e_i, e_j) = 0 \quad \text{if } j \neq i \pm 1.$$

Hence,

$$(v, v) = \sum_{i=1}^{k} i^2 - 2\sum_{i=1}^{k-1} \frac{1}{2} i(i+1) = k^2 - \sum_{i=1}^{k-1} i$$
$$= k^2 - \frac{k(k-1)}{2} = \frac{k(k+1)}{2}.$$

Proof of Proposition We need only prove (ii) and (iii).

Proof of (ii) Assume $m = 4$. We assume that the edge of order m lies in the "interior" of X. (Otherwise, we have B_ℓ). We want to show $X = F_4$. In the graph



we have $i \geq 2$ and $j = \ell - i \geq 2$. Let

$$v = e_1 + 2e_2 + \cdots + ie_i$$

$$w = e_\ell + 2e_{\ell-1} + \cdots + je_{i+1}.$$

Then

$$\|v\| = \frac{i(i+1)}{2} \quad \text{and} \quad \|w\| = \frac{j(j+1)}{2}$$

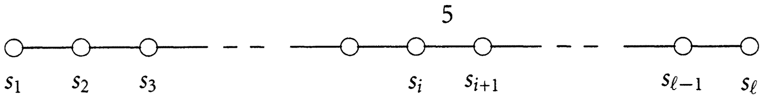
$$(v, w) = -ij(e_i, e_{i+1}) = -ij\cos\left(\frac{\pi}{4}\right) = -\frac{ij}{\sqrt{2}}.$$

We now invoke the trigonometric identity that $(v, w)^2 = \|v\|^2 \, \|w\|^2 \cos^2 \phi$, where ϕ is the angle between v and w. In our case, we have $\cos^2 \phi < 1$, and so $(v, w)^2 < \|v\|^2 \, \|w\|^2$. Substituting the above equalities, we obtain $\frac{i^2 j^2}{2} < \frac{ij(i+1)(j+1)}{4}$ and, hence,

$$2ij < (i+1)(j+1).$$

Since $i, j \geq 2$, this last inequality forces $i = j = 2$. So X is the F_4 graph.

Proof of (iii) Assume $m = 5$. We have the graph



Our argument is analogous to the previous one. Let $j = \ell - i$ and let

$$v = e_1 + 2e_2 + \cdots + ie_i$$
$$w = e_\ell + 2e_{\ell-1} + \cdots + je_{i+1}.$$

The inequality $(v, w)^2 < \|v\|^2 \, \|w\|^2$ gives $i^2 j^2 \cos^2(\frac{\pi}{5}) < \frac{ij(i+1)(j+1)}{4}$ and, hence,

$$(*) \qquad ij \cos^2\left(\frac{\pi}{5}\right) < \frac{ij(i+1)(j+1)}{4}.$$

Since $\cos(\frac{\pi}{5}) = \frac{1+\sqrt{5}}{4}$, we have

$$(**) \qquad \cos^2\left(\frac{\pi}{5}\right) = \frac{3+\sqrt{5}}{8} > \frac{5}{8}.$$

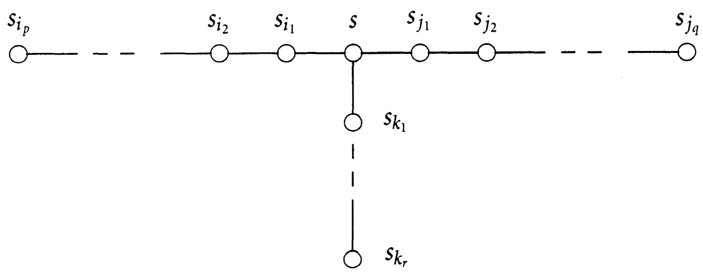
Combining $(*)$ and $(**)$, we obtain

$$\frac{5}{2} ij < (i+1)(j+1).$$

This inequality forces $i = 1$ or $j = 1$. And, if $i = 1$, then $j = 2$ or 3. So X is the H_3 or H_4 graph.

8-5 The ramification case

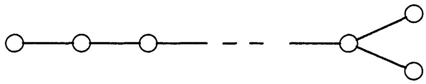
We now study case (i) of Proposition 8-3. Assume that X is a graph of the form



where $p \geq q \geq r$. In this section, we shall prove:

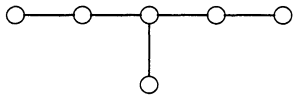
Proposition *X is one of the following:*

(i) p arbitrary, $q = r = 1$

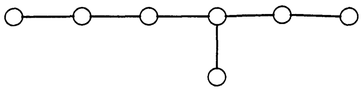


(D_ℓ)

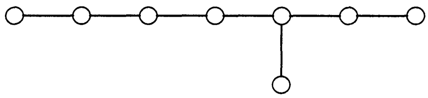
(ii) $p = 2, 3, 4$, $q = 2$, $r = 1$



(E_6)



(E_7)



(E_8)

The key to proving the proposition is the inequality

Lemma $\frac{1}{p+1} + \frac{1}{q+1} + \frac{1}{r+1} > 1.$

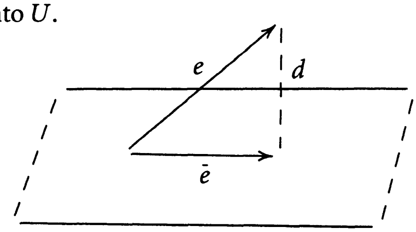
Proof We prove the lemma by using trigonometry. Let

$$u = e_{i_p} + 2e_{i_{p-1}} + \cdots + pe_{i_1}$$
$$v = e_{j_q} + 2e_{j_{q-1}} + \cdots + qe_{j_1}$$
$$w = e_{k_r} + 2e_{k_{r-1}} + \cdots + re_{k_1}.$$

Since the vertices of u, v and w come from the three distinct arms of X, we have $(u, v) = (u, w) = (v, w) = 0$. Thus

$$(*) \qquad \left\{ \frac{u}{\|u\|}, \frac{v}{\|v\|}, \frac{w}{\|w\|} \right\} \text{ are orthonormal.}$$

Let U be the three-dimensional vector space $U = \mathbb{R}\frac{u}{\|u\|} \oplus \mathbb{R}\frac{v}{\|v\|} \oplus \mathbb{R}\frac{w}{\|w\|}$. Let $e = e_s$, i.e., the vector corresponding to the ramified vertex s of the graph. Let $d =$ distance of e to U. In the following picture we have indicated d as well as $\bar{e} =$ the projection of e onto U.



It follows from the right-angled triangle in the picture that

$$(**) \qquad \|\bar{e}\|^2 + d^2 = \|e\|^2 = 1.$$

We now develop an alternative expression for $\bar{e}$ and substitute it into $(**)$. Because of $(*)$, we have

$$\bar{e} = \left(e, \frac{u}{\|u\|}\right) \frac{u}{\|u\|} + \left(e, \frac{v}{\|v\|}\right) \frac{v}{\|v\|} + \left(e, \frac{w}{\|w\|}\right) \frac{w}{\|w\|}.$$

So

$$\|\bar{e}\|^2 = \frac{(e,u)^2}{\|u\|^2} + \frac{(e,v)^2}{\|v\|^2} + \frac{(e,w)^2}{\|w\|^2}.$$

It follows from the length lemma in §8-4 that

$$\|u\|^2 = \frac{1}{2}p(p+1), \quad \|v\|^2 = \frac{1}{2}q(q+1) \quad \text{and} \quad \|w\|^2 = \frac{1}{2}r(r+1).$$

Since e is orthogonal to all vertices except e_{i_1}, e_{j_1} and e_{k_1}, we also have

$$(e,u) = -\frac{1}{2}p, \, (e,v) = -\frac{1}{2}q \quad \text{and} \quad (e,w) = -\frac{1}{2}r.$$

Combining all the above, we have

$$(***) \qquad \|\bar{e}\|^2 = \frac{1}{2}\frac{p}{p+1} + \frac{1}{2}\frac{q}{q+1} + \frac{1}{2}\frac{r}{r+1}.$$

We now merge $(**)$ and $(***)$, and prove the lemma. From $(**)$, we have the inequality

$$1 - \|\bar{e}\|^2 = d^2 > 0.$$

Substituting $(***)$, we have

$$1 - \frac{1}{2}\frac{p}{p+1} - \frac{1}{2}\frac{q}{q+1} - \frac{1}{2}\frac{r}{r+1} > 0,$$

whence the inequality of the lemma easily follows because $1-\alpha > 0$ and $2\alpha+\beta = 3$ imply that $\beta > 1$. ■

Proof of Proposition First of all, we must have

$$r = 1$$

because the inequality of the lemma, plus $p \geq q \geq r$, gives $\frac{3}{r+1} > 1$. Secondly, we must have

$$q = 1, 2.$$

For, since $r = 1$, the inequality of the lemma becomes $\frac{1}{p+1} + \frac{1}{q+1} > \frac{1}{2}$. And, since $p \geq q$, we have $\frac{2}{q+1} > \frac{1}{2}$. We consider separately the two cases for q.

(i) If $q = 1$, then p is arbitrary because $q = 1$ means that the inequality of the lemma becomes

$$\frac{1}{p+1} > 0.$$

This inequality imposes no restrictions on p.

(ii) If $q = 2$, then $p = 2, 3, 4$ because we have $p \geq q \geq 2$, and the inequality of the lemma becomes

$$\frac{1}{p+1} > \frac{1}{6}.$$

8-6 Coxeter graphs of root systems

We are left verifying Theorem 8-1B. We have to show that, for each of the Coxeter graphs listed in Theorem 8-1A, there is a finite Euclidean reflection group that gives rise to the Coxeter graph (= Coxeter system). Finite reflection groups arise from root systems. So it suffices to look for an appropriate root system. This actually simplifies the process, since the Coxeter graph (= Coxeter system) associated with a root system is easy to determine.

Coxeter Graph of a Root System Let Δ be a root system. Given a fundamental system $\Sigma = (\alpha_1, \ldots, \alpha_\ell)$ of Δ, then, for each $1 \leq i < j \leq \ell$, $\frac{(\alpha_i,\alpha_j)}{\|\alpha_i\|\,\|\alpha_j\|} = -\cos(\frac{\pi}{m_{ij}})$ for some $m_{ij} \in \mathbb{Z}^+$. We then assign a Coxeter graph X to Δ by the rules:

(i) $\Sigma =$ the vertices of X;
(ii) Given $\alpha_i \neq \alpha_j \in \Sigma$, there is no edge between α_i and α_j if $m_{ij} = 2$ (i.e., α_i and α_j are at right angles);
(iii) Given $\alpha_i \neq \alpha_j \in \Sigma$, there is an edge labelled by m_{ij} if $m_{ij} \geq 3$.

The Coxeter graph of Δ has the desired relation to the Coxeter graph of $W(\Delta)$.

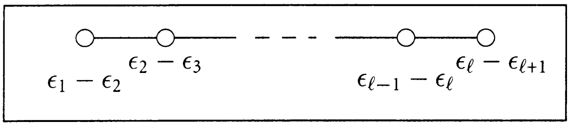
Lemma *The Coxeter graph of Δ = the Coxeter graph of $W(\Delta)$.*

Proof The vertices $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$ and $S = \{s_{\alpha_1}, \ldots, s_{\alpha_\ell}\}$ are in one-to-one correspondence. Moreover, this correspondence respects the assigning of edges because there is an edge between α_i and α_j of order m if and only if $\frac{(\alpha_i,\alpha_j)}{\|\alpha_i\|\,\|\alpha_j\|} = -\cos(\frac{\pi}{m})$, whereas there is an edge between s_{α_i} and s_{α_j} of order m if and only if $s_{\alpha_i}s_{\alpha_j}$ has order m. And, as in property (C-2) of §6-3, $s_{\alpha_i}s_{\alpha_j}$ has order m if and only if $\frac{(\alpha_i,\alpha_j)}{\|\alpha_i\|\,\|\alpha_j\|} = \cos(\pi - \frac{\pi}{m}) = -\cos(\frac{\pi}{m})$. ∎

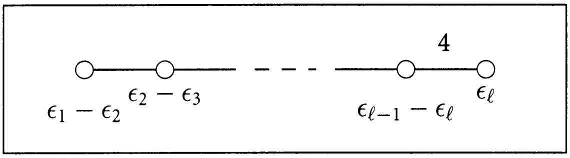
So the Coxeter graph of a root system tells us precisely what Coxeter group we obtain from it. We now list root systems that have the Coxeter graphs listed in Theorem 8-1A as their graphs. In each case, in order to make the correspondence explicit, we give the Coxeter graph with the vertices labelled by fundamental roots. In all that follows, let $\{\epsilon_i\}$ be an orthonormal basis of $\mathbb{E} = \mathbb{R}^\ell$ or $\mathbb{R}^{\ell+1}$.

Root Systems

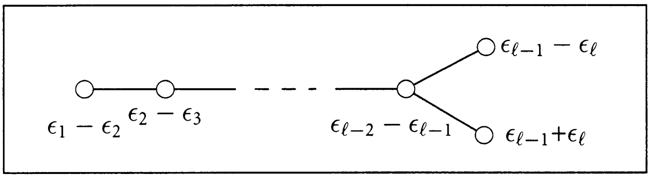
(a) The root system $A_\ell = \{\epsilon_i - \epsilon_j \mid i \neq j, 1 \leq i, j \leq \ell + 1\}$:



(b) The root system $B_\ell = \{\pm\epsilon_i \mid 1 \leq i \leq \ell\} \coprod \{\pm\epsilon_i \pm \epsilon_j \mid 1 \leq i < j \leq \ell\}$:



(c) The root system $D_\ell = \{\pm\epsilon_i \pm \epsilon_j \mid 1 \leq i < j \leq \ell\}$:

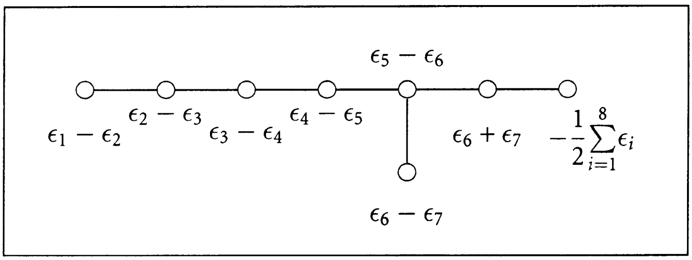


We shall treat the root systems E_6, E_7 and E_8 in the order: E_8, E_7, E_6. For E_6 and E_7 are subroot systems of E_8.

(d) The root system $E_8 = \Delta_1 \coprod \Delta_2$, where

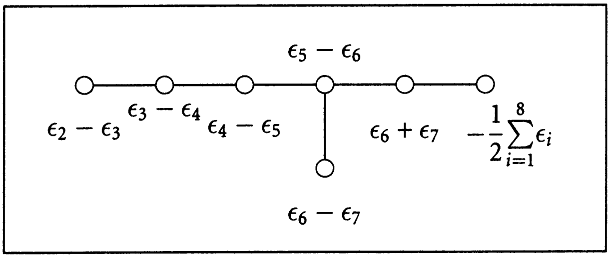
$$\Delta_1 = \{\pm\epsilon_i \pm \epsilon_j \mid 1 \leq i < j \leq 8\}$$

$$\Delta_2 = \left\{ \frac{1}{2} \sum_{i=1}^{8} \lambda_i \epsilon_i \;\middle|\; \lambda_i = \pm 1 \text{ and } \prod_{i=1}^{8} \lambda_i = 1 \right\}$$



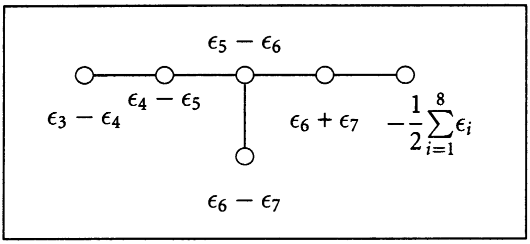
(e) The root system $E_7 = \Delta_1 \coprod \Delta_2 \coprod \Delta_3$, where

$$\Delta_1 = \{\pm\epsilon_i \pm \epsilon_j \mid 2 \le i < j \le 7\}$$
$$\Delta_2 = \{\pm(\epsilon_1 + \epsilon_8)\}$$
$$\Delta_3 = \left\{ \pm\frac{1}{2}\sum_{i=1}^{8} \lambda_i\epsilon_i \;\middle|\; \lambda_i = \pm 1, \lambda_1 = \lambda_8 = 1, \prod_{i=1}^{8} \lambda_i = 1 \right\}$$



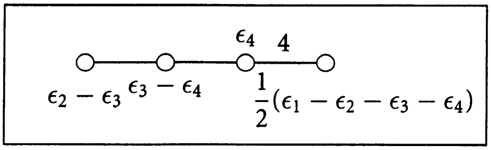
(f) The root system $E_6 = \Delta_1 \coprod \Delta_2$, where

$$\Delta_1 = \{\pm\epsilon_i \pm \epsilon_j \mid 3 \le i < j \le 7\}$$
$$\Delta_2 = \left\{ \pm\frac{1}{2}\sum_{i=1}^{8} \lambda_i\epsilon_i \;\middle|\; \lambda_i = \pm 1, \lambda_1 = \lambda_2 = \lambda_8 = 1, \prod_{i=1}^{8} \lambda_i = 1 \right\}$$

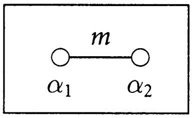


(g) The root system $F_4 = \Delta_1 \coprod \Delta_2 \coprod \Delta_3$, where

$$\Delta_1 = \{\pm\epsilon_i \mid 1 \le i \le 4\}$$
$$\Delta_2 = \{\pm\epsilon_i \pm \epsilon_j \mid 1 \le i < j \le 4\}$$
$$\Delta_3 = \left\{ \frac{1}{2}(\pm\epsilon_1 \pm \epsilon_2 \pm \epsilon_3 \pm \epsilon_4) \right\}$$



(h) The root system $G_2(m) = \{(\cos(\frac{k\pi}{m}), \sin(\frac{k\pi}{m})) \mid 0 \leq k \leq 2m-1\}$



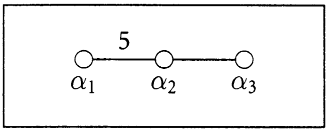
and $\alpha_1 = (\cos(\frac{\pi}{m}), \sin(\frac{\pi}{m}))$ and $\alpha_2 = (\cos(\frac{2\pi}{m}), \sin(\frac{2\pi}{m}))$.

In the case of our last two root systems, we shall let $\beta = \cos(\frac{\pi}{5})$.

(i) The root system $H_3 = \Delta_1 \coprod \Delta_2$, where

$$\Delta_1 = \{\pm\epsilon_i \mid 1 \leq i \leq 3\}$$

$$\Delta_2 = \left\{\text{all even permutations of } \left(\pm\left(\beta + \frac{1}{2}\right), \pm\beta, \pm\frac{1}{2}\right)\right\}$$



and

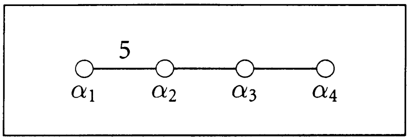
$$\alpha_1 = \left(\frac{1}{2} + \beta, \beta, -\frac{1}{2}\right), \quad \alpha_2 = \left(-\frac{1}{2} - \beta, \beta, \frac{1}{2}\right) \quad \text{and}$$

$$\alpha_3 = \left(\frac{1}{2}, -\frac{1}{2} - \beta, \beta\right).$$

(j) The root system $H_4 = \Delta_1 \coprod \Delta_2$, where

$$\Delta_1 = \{\pm\epsilon_i \mid 1 \leq i \leq 4\} \coprod \left\{\frac{1}{2}(\pm 1, \pm 1, \pm 1, \pm 1)\right\}$$

$$\Delta_2 = \left\{\text{all even permutations of } \left(\pm\left(\beta + \frac{1}{2}\right), \pm\beta, \pm\frac{1}{2}, 0\right)\right\}$$



and

$$\alpha_1 = \left(\frac{1}{2} + \beta, \beta, -\frac{1}{2}, 0\right) \quad \text{and} \quad \alpha_2 = \left(-\frac{1}{2} - \beta, \beta, \frac{1}{2}, 0\right)$$

$$\alpha_3 = \left(\frac{1}{2}, -\frac{1}{2} - \beta, \beta, 0\right) \quad \text{and} \quad \alpha_4 = \left(-\frac{1}{2}, 0, -\frac{1}{2} - \beta, \beta\right).$$

As a final comment, the root systems presented above have their own history. Most of them, namely the crystallographic ones, arose as the root systems associated with semisimple Lie algebras. See Appendix D for a discussion of this relation. The crystallographic root systems are discussed and classified in Chapter 10. The classification of finite reflection groups/Coxeter systems presented in this section is a modification of that classification.

III Weyl groups

The next five chapters study a refinement of finite reflection groups. Weyl groups are finite Euclidean reflection groups defined over $\mathbb{Z}$, not just over $\mathbb{R}$. Alternatively, they are reflection groups possessing special types of root systems, namely "crystallographic" root systems. The classification of Weyl groups is a refinement of that obtained for finite reflection groups.

Not surprisingly, the concepts and results from Chapters 1 through 8, where Euclidean reflection groups were studied and classified, play a major role in the analysis of Weyl groups. But we should point out a difference in emphasis. Previously, the root system was a tool used to understand the associated reflection group. In the Weyl case, root systems will become much more the primary object of study. Crystallographic root systems are rigid enough to be classified, and the classification of Weyl groups reduces to the classification of crystallographic root systems.

In Chapters 9 and 10, we are concerned with classifying Weyl groups and crystallographic root systems. In Chapter 11, we define and study affine Weyl groups. In Chapter 12, we study closed root systems. In Chapter 13, we establish a polynomial identity over $\mathbb{Z}$ relating length in a Weyl group with height in its underlying crystallographic root system.

9 Weyl groups

Weyl groups are *integral forms* for finite Euclidean reflection groups. Their data consist of the reflection group structure, plus a lattice in Euclidean space that is stable under the group action. In this chapter, we shall show that a reflection group has such an equivariant lattice if and only if it has a crystallographic root system. Moreover, a definite relation will also be established between the crystallographic root system and the possible equivariant lattices. This, then, reduces the classification of Weyl groups to that of crystallographic root systems, and that classification will be carried out in the next chapter.

9-1 Weyl groups

A *lattice (of rank ℓ)* is a free $\mathbb{Z}$ module $\mathcal{L} = \mathbb{Z}^{\ell}$. Group actions

$$W \times \mathcal{L} \to \mathcal{L}$$

on lattices are analogous to group actions on vector spaces as defined in Appendix B. We have a group action with the requirement that, for each $\varphi \in W$, the induced map $\varphi\colon \mathcal{L} \to \mathcal{L}$ is a $\mathbb{Z}$-linear map. A lattice with an action of the group W will be called a *W-equivariant lattice.*

Definition: A *Weyl group* is a finite Euclidean reflection group $W \subset O(\mathbb{E})$ admitting a W-equivariant lattice $\mathcal{L} \subset \mathbb{E}$, where $\mathbb{E} = \mathcal{L} \otimes_{\mathbb{Z}} \mathbb{R}$.

So the action of W on $\mathbb{E}$ is determined by its action on $\mathcal{L}$. We say that a Weyl group is *reducible* or *irreducible* if it is reducible or irreducible as a finite reflection group. It will be confirmed at the end of §9-5 that, in such a decomposition $W = W_1 \times W_2$, the two reflection groups W_1 and W_2 must also be Weyl groups.

Given a fixed reflection group $W \subset O(\mathbb{E})$, we want to classify the W-equivariant lattices $\mathcal{L} \subset \mathbb{E}$ such that $\mathbb{E} = \mathcal{L} \otimes_{\mathbb{Z}} \mathbb{R}$ up to an appropriate equivalence. Given W-equivariant lattices $\mathcal{L}, \mathcal{L}'$, a *$W$-equivariant map* $f\colon \mathcal{L} \to \mathcal{L}'$ is a $\mathbb{Z}$-linear map such that, for all $\varphi \in W$, the following diagram commutes:

$$\begin{tikzcd}
\mathcal{L} \arrow[r, "f"] \arrow[d, "\varphi"] & \mathcal{L}' \arrow[d, "\varphi"] \\
\mathcal{L} \arrow[r, "f"] & \mathcal{L}'
\end{tikzcd}$$

We say that two W-equivariant lattices $\mathcal{L}$ and $\mathcal{L}'$ are *isomorphic* if there exists a W-equivariant linear isomorphism $f\colon \mathcal{L} \xrightarrow{\cong} \mathcal{L}'$.

The rest of this chapter is concerned with the classification of irreducible Weyl groups up to isomorphism. We already have a classification of finite (irreducible, essential) Euclidean reflection groups. We shall proceed by refining that classification. For each finite Euclidean reflection group $W \subset O(\mathbb{E})$ we should like to determine, up to isomorphism, all the possible W-equivariant lattices $\mathcal{L} \subset \mathbb{E}$ such

that $\mathcal{L} \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{E}$. It is possible that a particular reflection group $W \subset O(\mathbb{E})$ possesses no such W-equivariant lattice $\mathcal{L} \subset \mathbb{E}$ (i.e., is not a Weyl group) and it is also possible that it contains many (i.e., is a Weyl group in more ways than one). (This second fact is parallel to the fact that subgroups of $\mathrm{GL}_\ell(\mathbb{Z})$ that are not conjugate in $\mathrm{GL}_\ell(\mathbb{Z})$ may be conjugate in $\mathrm{GL}_\ell(\mathbb{Z})$.)

So there are two questions to consider about Weyl groups:

(i) We want to determine which finite reflection groups $W \subset O(\mathbb{E})$ admit a W-equivariant lattice $\mathcal{L} \subset \mathbb{E}$, such that $\mathcal{L} \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{E}$.
(ii) For each such W, we want to determine all the distinct (i.e., nonisomorphic) equivariant lattices $\mathcal{L} \subset \mathbb{E}$.

The rest of this chapter will begin to answer these questions by exploring the relation between Weyl groups and crystallographic root systems. It will be demonstrated that a reflection group $W \subset O(\mathbb{E})$ is a Weyl group if and only if it possesses a crystallographic root system $\Delta \subset \mathbb{E}$. Notably, crystallographic root systems give rise, in a canonical way, to W-equivariant lattices $\mathcal{L} \subset \mathbb{E}$. In the next three sections, we construct lattices $\mathcal{Q} \subset \mathcal{P} \subset \mathbb{E}$, called the *root lattice* and the *weight lattice*, respectively, which are associated with any crystallographic root system $\Delta \subset \mathbb{E}$. Both these lattices, as well as any intermediary lattice $\mathcal{Q} \subseteq \mathcal{L} \subseteq \mathcal{P}$, will turn out to be W- (Δ-) equivariant. Moreover, the collection $\{\mathcal{L} \mid \mathcal{Q} \subseteq \mathcal{L} \subseteq \mathcal{P}\}$ will also turn out to be (up to isomorphism) the complete set of W- (Δ-) equivariant lattices. Thus the classification of Weyl groups is a refinement of the classification of crystallographic root systems. The latter classification will be given in Chapter 10. So by the end of Chapter 10, we shall have achieved a complete classification of Weyl groups.

Throughout our discussion of Weyl groups, *we shall only be dealing with the case of essential reflection groups and essential root systems.* As we shall see, this property guarantees that the root and weight lattices satisfy $\mathcal{Q} \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{E}$ and $\mathcal{P} \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{E}$. Indeed, this property is needed even to properly define $\mathcal{P}$. We also remark that essential crystallographic root systems are of very significant interest because of the correspondence constructed in Appendix D for Lie theory. Such root systems are precisely the root systems arising from semisimple Lie algebras, and are used to classify them.

As far as investigating question (i) above is concerned, the above assumption is not really a restriction. The classification of finite reflection groups produced in Chapter 8 holds up to stable isomorphism; and every stable isomorphism class is uniquely represented by an essential reflection group. It is also not hard to see that, if one member of a stable isomorphism class possesses an equivariant lattice, then every member must.

On the other hand, when we turn to investigating question (ii), then restricting to the essential case is a genuine restriction because not all examples of W-equivariant lattices can be determined from the essential case, i.e., they are not direct sums of these cases. We are definitely ignoring extra complexities. From the vantage point of representation theory, this ie exactly the phenomenon that there are representations over $\mathbb{Z}$ that are not a direct sum of simple representations.

Example: Consider the group $W = \mathbb{Z}/2\mathbb{Z}$ and let $\tau \neq 1$ be the involution generating the group. The reflection group $W \subset \mathrm{GL}_2(\mathbb{R})$ given by $\tau = \left[\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ admits two different (i.e., nonisomorphic) W-equivariant lattices. For, if we write $\mathcal{L} = \mathbb{Z}x \oplus \mathbb{Z}y$, then different actions of τ on $\mathcal{L}$ are given by

$$\tau \cdot x = -x \quad \text{and} \quad \tau \cdot y = y,$$

and by

$$\tau \cdot x = y \quad \text{and} \quad \tau \cdot y = x.$$

When we pass to $\mathcal{L} \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{R}^2$, both actions are equivalent, and each produces the above reflection group $W \subset \mathrm{GL}_2(\mathbb{R})$. Thus they are integral forms of the same reflection group. But in the first case τ is diagonalizable, whereas in the second it is not. So the second case is one of the extra complexities raised in the previous paragraph. It does not decompose as a direct sum.

Notation: We recall notation associated with crystallographic root systems. For each $x, y \in \mathbb{E}$, let

$$\langle x, y \rangle = \frac{2(x, y)}{(x, x)}.$$

The fact that

$$\langle \alpha, \beta \rangle \in \mathbb{Z} \quad \text{for all } \alpha, \beta \in \Delta$$

is the special property possessed by crystallographic root systems. Property (A-1) of §1-1 can be reformulated as asserting that the reflection s_α is defined by

$$s_\alpha \cdot x = x - \langle \alpha, x \rangle \alpha.$$

We shall use the $\langle x, y \rangle$ notation throughout the treatment of Weyl groups and crystallographic root systems.

9-2 The root lattice $\mathcal{Q}$

Let $\Delta \subset \mathbb{E}$ be an essential crystallographic root system. The next three sections are devoted to the construction of certain canonical W- (Δ-) equivariant lattices associated with Δ. We define the *root lattice of* Δ as

$$\mathcal{Q} = \mathcal{Q}(\Delta) = \text{all } \mathbb{Z}\text{-linear combinations in } \mathbb{E} \text{ of the elements of } \Delta.$$

The root lattice satisfies the following properties:

(i) $\mathcal{Q} = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_\ell$ for any fundamental system $\{\alpha_1, \ldots, \alpha_\ell\}$ of Δ.
(ii) $\mathcal{Q}$ is W- (Δ-) equivariant.

To justify these two facts, we let

$$\mathcal{L} = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_\ell \subset \mathcal{Q}.$$

First of all, $\mathcal{L}$ is W- (Δ-) equivariant because $\{s_{\alpha_1}, \dots, s_{\alpha_\ell}\}$ generate $W(\Delta)$ (see §4-1) and $s_{\alpha_i} \cdot \alpha_j = \alpha_j - \langle \alpha_i, \alpha_j \rangle \alpha_i$, where $\langle \alpha_i, \alpha_j \rangle \in \mathbb{Z}$. Secondly, as we observed in §3-6, every $\alpha \in \Delta$ is of the form $\alpha = \varphi \cdot \alpha_i$ for some $\varphi \in W(\Delta)$ and some fundamental root α_i. Thus $\alpha \in \mathcal{L}$. It follows that $\mathcal{Q} \subset \mathcal{L}$, and so $\mathcal{L} = \mathcal{Q}$.

The fact that $\Delta \subset \mathbb{E}$ is essential is equivalent to asserting that $\mathcal{Q} \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{E}$. The root lattice is not the only W- (Δ-) equivariant lattice $\mathcal{L} \subset \mathbb{E}$ such that $\mathcal{L} \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{E}$. We shall continue to construct such lattices in the next two sections.

9-3 Coroots and the coroot lattice $\mathcal{Q}^\vee$

Let $\Delta = \{\alpha\}$ be an essential crystallographic root system. For each $\alpha \in \Delta$, we have the *coroot*

$$\alpha^\vee = \frac{2\alpha}{(\alpha, \alpha)}.$$

Proposition A *The coroots $\Delta^\vee = \{\alpha^\vee\}$ form a crystallographic root system.*

The first property of a root system

(B-1) Given $\alpha^\vee \in \Delta^\vee$, then $\lambda\alpha^\vee \in \Delta$ if and only if $\lambda = \pm 1$

follows easily from the corresponding properties for Δ (we are merely altering each α by the scalar $2/(\alpha, \alpha)$. The crystallographic property

(B-3) $\langle \alpha^\vee, \beta^\vee \rangle \in \mathbb{Z}$ for all $\alpha^\vee, \beta^\vee \in \Delta^\vee$

is also a straightforward translation of the crystallographic property for Δ because if we substitute $\alpha^\vee = 2\alpha/(\alpha, \alpha)$ and $\beta^\vee = 2\beta/(\beta, \beta)$, we obtain the identity

$$2(\alpha^\vee, \beta^\vee)/(\alpha^\vee, \alpha^\vee) = 2(\alpha, \beta)/(\beta, \beta).$$

So $\langle \alpha^\vee, \beta^\vee \rangle = \langle \beta, \alpha \rangle \in \mathbb{Z}$. Lastly, we have the invariance property

(B-2) $s_{\alpha^\vee} \cdot \beta^\vee \in \Delta^\vee$ for all $\alpha^\vee, \beta^\vee \in \Delta^\vee$.

First of all, observe that $s_\alpha = s_{\alpha^\vee}$ for all $\alpha \in \Delta$. (The observation was made in §1-1 that $s_\alpha = s_{k\alpha}$ for all $0 \neq k \in \mathbb{R}$.) Thus

$$W(\Delta) = W(\Delta^\vee)$$

as reflection groups. To finish the proof of (B-2) it suffices to show:

Lemma *The coroots $\Delta^\vee$ are permuted by $W(\Delta)$.*

Proof Given $\alpha^\vee \in \Delta^\vee$ and $\varphi \in W(\Delta)$, we have

$$\varphi \cdot (\alpha^\vee) = \varphi \cdot \left(\frac{2\alpha}{(\alpha, \alpha)} \right) = \frac{2\varphi \cdot \alpha}{(\alpha, \alpha)} = \frac{2\varphi \cdot \alpha}{(\varphi \cdot \alpha, \varphi \cdot \alpha)} = (\varphi \cdot \alpha)^\vee. \qquad \blacksquare$$

As an extension of the root properties of $\Delta^\vee$, we also have:

Proposition B *For any fundamental system $\Sigma = \{\alpha_1, \dots, \alpha_\ell\}$ of Δ, $\Sigma^\vee = \{\alpha_1^\vee, \dots, \alpha_\ell^\vee\}$ is a fundamental system of $\Delta^\vee$.*

Proof We need to show that every $\alpha^\vee \in \Delta^\vee$ can be expanded in terms of $\Sigma^\vee$ with every coefficient ≥ 0, or every coefficient ≤ 0. This property holds for the expansion of each $\alpha \in \Delta$ in terms of Σ. Write

$$\alpha = \sum_i \lambda_i \alpha_i.$$

The identities $\alpha^\vee = 2\alpha/(\alpha, \alpha)$ and $\alpha_i^\vee = 2\alpha_i/(\alpha_i, \alpha_i)$ then give

$$\alpha^\vee = \sum_i \frac{(\alpha_i, \alpha_i)}{(\alpha, \alpha)} \lambda_i \alpha_i^\vee.$$

So we have merely altered the coefficients λ_i by positive multiples. ■

Example: Consider the root systems B_ℓ and C_ℓ. Let $\{\epsilon_1, \ldots, \epsilon_\ell\}$ be an orthonormal basis of $\mathbb{R}^\ell$. Then the B_ℓ root system is given by

$$\Delta = \{\pm\epsilon_i \pm \epsilon_j\} \coprod \{\pm\epsilon_i\}.$$

So

$$\Delta^\vee = \{\pm\epsilon_i \pm \epsilon_j\} \coprod \{\pm 2\epsilon_i\}$$

which is the C_ℓ root system. Thus $B_\ell^\vee = C_\ell$. Conversely, $C_\ell^\vee = B_\ell$.

For most crystallographic root systems, we have $\Delta^\vee = \Delta$. An examination of the irreducible crystallographic root systems listed in §10-5 yields that $\Delta^\vee$ is distinct from Δ only in the cases $\Delta = B_\ell$ and $\Delta = C_\ell$, which were discussed above.

Nevertheless, coroots are an important theoretical concept. Notably, the coroots of Δ determine the coroot lattice of Δ that plays an important part in the analysis of both the Weyl group and the affine Weyl group of Δ. Let Δ be a crystallographic root system. We define the *coroot lattice* as:

$$\begin{aligned} \mathcal{Q}^\vee &= \text{the root lattice of the root system } \Delta^\vee \\ &= \text{all } \mathbb{Z}\text{-linear combinations of the elements of } \Delta^\vee. \end{aligned}$$

It follows from the previous results of this section that:

(i) $\mathcal{Q}^\vee = \mathbb{Z}\alpha_1^\vee \oplus \cdots \oplus \mathbb{Z}\alpha_\ell^\vee$ for any fundamental system $\{\alpha_1, \ldots, \alpha_\ell\}$ of Δ;
(ii) $\mathcal{Q}^\vee$ is $W(\Delta) = W(\Delta^\vee)$ equivariant.

Also, Δ is essential implies $\mathcal{Q}^\vee \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{E}$.

9-4 Fundamental weights and the weight lattice $\mathcal{P}$

The weight lattice $\mathcal{P}$ is, by definition, the dual of the coroot lattice $\mathcal{Q}^v$. Given a lattice $\mathcal{L} \subset \mathbb{E}$, where $\mathcal{L} \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{E}$, we define the *dual lattice* as

$$\mathcal{L}^{\perp} = \{x \in \mathbb{E} \mid (x, y) \in \mathbb{Z} \text{ for all } y \in \mathcal{L}\}.$$

If $\mathcal{L} = \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_\ell$, then $\mathcal{L}^{\perp} = \mathbb{Z}y_1 \oplus \cdots \oplus \mathbb{Z}y_\ell$, where $(x_i, y_j) = \delta_{ij}$.

Let $\Delta \subset \mathbb{E}$ be an essential crystallographic root system. So $\mathcal{Q} \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{E}$ and $\mathcal{Q}^v \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{E}$, where $\mathcal{Q}$ and $\mathcal{Q}^v$ are the root and coroot lattices of Δ. The *weight lattice* $\mathcal{P}$ of Δ is the dual lattice of $\mathcal{Q}^v$. More directly, because of the identities

$$\langle \alpha, x \rangle = \frac{2(\alpha, x)}{(\alpha, \alpha)} = (\alpha^v, x),$$

we can define $\mathcal{P}$ by

$$\mathcal{P} = \{x \in \mathbb{E} \mid \langle \alpha, x \rangle \in \mathbb{Z} \text{ for all } \alpha \in \Delta\}.$$

Observe that the crystallographic condition for Δ forces

$$\mathcal{Q} \subset \mathcal{P}.$$

This inclusion is discussed further at the end of the section.

Given the fundamental system $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$ of Δ and, hence, the fundamental system $\Sigma^v = \{\alpha_1^v, \ldots, \alpha_\ell^v\}$ of Δ^v, then the *fundamental weights* $\{\omega_1, \ldots, \omega_\ell\}$ (with respect to Σ) are defined by

$$(\alpha_i^v, \omega_j) = \delta_{ij}.$$

Since $\mathcal{Q}^v = \mathbb{Z}\alpha_1^v \oplus \cdots \oplus \mathbb{Z}\alpha_\ell^v$, we have

$$\mathcal{P} = \mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_\ell$$

for the corresponding set of fundamental weights. Since the inner product $(\_, \_)$ and the lattice $\mathcal{Q}^v$ are both invariant under W, it follows that $\mathcal{P}$ is mapped to itself by W. For, given $x \in \mathcal{P}$ and $\varphi \in W$, then, for any $y \in \mathcal{Q}^v$, we have $(\varphi \cdot x, y) = (x, \varphi^{-1} \cdot y) \in \mathbb{Z}$. So $\varphi \cdot x \in \mathcal{P}$.

Examples: In the following examples we use the notation from §2-4.

(a) Root System A_ℓ We have $\Delta \subset \mathbb{E}$, where $\{\epsilon_1, \epsilon_2, \ldots, \epsilon_{\ell+1}\}$ is an orthonormal basis of $\mathbb{R}^{\ell+1}$, and

$$\mathbb{E} = \left\{\sum_{i=1}^{\ell+1} c_i\epsilon \;\middle|\; c_i \in \mathbb{R}, \sum c_i = 0\right\}$$

$$\Delta = \{\epsilon_i - \epsilon_j \mid i \neq j,\ 0 \leq i, j \leq \ell\}.$$

A fundamental system for Δ is

$$\Sigma = \{\epsilon_1 - \epsilon_2, \epsilon_2 - \epsilon_3, \ldots, \epsilon_\ell - \epsilon_{\ell+1}\}.$$

So $\Delta^v = \Delta$, $\Sigma^v = \Sigma$ and the fundamental weights (with respect to Σ) are $\{\omega_1, \ldots, \omega_\ell\}$, where

$$\omega_k = \epsilon_1 + \cdots + \epsilon_k - \frac{k}{\ell+1}(\epsilon_1 + \cdots + \epsilon_{\ell+1}).$$

Observe that the coroots $\{\epsilon_i - \epsilon_{i+1}\}$ and the elements $\{\epsilon_1 + \cdots + \epsilon_i\}$ are dual to each other, i.e.,

$$(\epsilon_i - \epsilon_{i+1}, \epsilon_1 + \cdots + \epsilon_k) = \delta_{ik},$$

whereas the element $\epsilon_1 + \cdots + \epsilon_{\ell+1}$ pairs off trivially with all of the coroots. Linear combinations of these elements $\{\omega_k\}$ are then chosen to satisfy the constraints of the subspace $\mathbb{E} \subset \mathbb{R}^{\ell+1}$.

***(b) Root System** B_ℓ* Let $\{\epsilon_1, \ldots, \epsilon_\ell\}$ be a orthonormal basis of $\mathbb{R}^\ell$. Then the B_ℓ root system is given by

$$\Delta = \{\pm\epsilon_i \pm \epsilon_j\} \coprod \{\pm\epsilon_i\}.$$

As already observed in §9-2, the coroots

$$\Delta^v = \{\pm\epsilon_i \pm \epsilon_j\} \coprod \{\pm 2\epsilon_i\}$$

form the C_ℓ root system. Given a fundamental system

$$\Sigma = \{\epsilon_1 - \epsilon_2, \ldots, \epsilon_{\ell-1} - \epsilon_\ell, \epsilon_\ell\}$$

of Δ, then

$$\Sigma^v = \{\epsilon_1 - \epsilon_2, \ldots, \epsilon_{\ell-1} - \epsilon_\ell, 2\epsilon_\ell\}.$$

So the fundamental weights (with respect to Σ) are

$$\omega_k = \epsilon_1 + \cdots + \epsilon_k \quad \text{for } 1 \leq k < \ell$$
$$\omega_\ell = \frac{1}{2}(\epsilon_1 + \cdots + \epsilon_\ell).$$

***(c) Root Systems** C_ℓ* This time we have

$$\Delta = \{\pm\epsilon_i \pm \epsilon_j\} \coprod \{\pm 2\epsilon_i\},$$

with fundamental system

$$\Sigma = \{\epsilon_1 - \epsilon_2, \ldots, \epsilon_{\ell-1} - \epsilon_\ell, 2\epsilon_\ell\}.$$

Hence,

$$\Sigma^\vee = \{\epsilon_1 - \epsilon_2, \ldots, \epsilon_{\ell-1} - \epsilon_\ell, \epsilon_\ell\}$$

and the fundamental weights (with respect to Σ) are

$$\omega_k = \epsilon_1 + \cdots + \epsilon_k \quad \text{for } 1 \le k \le \ell.$$

(d) Root System D_ℓ If $\{\epsilon_1, \ldots, \epsilon_\ell\}$ is an orthonormal basis of $\mathbb{R}^\ell$, then we have

$$\Delta = \{\pm\epsilon_i \pm \epsilon_j\}$$

with fundamental system

$$\Sigma = \{\epsilon_1 - \epsilon_2, \ldots, \epsilon_{\ell-1} - \epsilon_\ell, \epsilon_{\ell-1} + \epsilon_\ell\}.$$

We have $\Delta^\vee = \Delta$ and $\Sigma^\vee = \Sigma$. So the fundamental weights are

$$\omega_k = \epsilon_1 + \cdots + \epsilon_k \quad \text{for } 1 \le k \le \ell - 2$$

$$\omega_{\ell-1} = \frac{1}{2}(\epsilon_1 + \cdots + \epsilon_{\ell-1} - \epsilon_\ell)$$

$$\omega_\ell = \frac{1}{2}(\epsilon_1 + \cdots + \epsilon_{\ell-1} + \epsilon_\ell).$$

Remark: It was pointed out previously that we have an inclusion $\mathcal{Q} \subset \mathcal{P}$. We close this section by describing this inclusion in detail. Since both lattices have the same rank, $\mathcal{Q}$ has finite index in $\mathcal{P}$. The *Cartan matrix* $[(\alpha_i^\vee, \alpha_j)]_{\ell\times\ell}$ tells us how to expand $\{\alpha_1, \ldots, \alpha_\ell\}$ in terms of $\{\omega_1, \ldots, \omega_\ell\}$. So $\det[(\alpha_i^\vee, \alpha_j)]$ gives the index of $\mathcal{Q}$ in $\mathcal{P}$, i.e., the order of the quotient group $\mathcal{P}/\mathcal{Q}$. A classification of irreducible crystallographic root systems is given in §10-5. The following chart gives the index of $\mathcal{Q}$ in $\mathcal{P}$ for all these irreducible crystallographic root systems.

Δ_ℓ	A_ℓ	B_ℓ	C_ℓ	D_ℓ	E_6	E_7	E_8	F_4	G_2
$\lvert\mathcal{P}/\mathcal{Q}\rvert$	$\ell + 1$	2	2	4	3	2	1	1	1

With the exception of D_ℓ, the quotient $\mathcal{P}/\mathcal{Q}$ is a cyclic group of the order given in the chart. In the case of D_ℓ, the quotient $\mathcal{P}/\mathcal{Q}$ is $\mathbb{Z}/4\mathbb{Z}$ for ℓ odd and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ for ℓ even.

9-5 Equivariant lattices

Let $W \subset O(\mathbb{E})$ be a finite essential Euclidean reflection group. In this section, we explain how to determine all the distinct W-equivariant lattices $\mathcal{L} \subset \mathbb{E}$ such that $\mathcal{L} \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{E}$. We shall demonstrate that all these lattices arise out of crystallographic root systems: there is a crystallographic root system Δ such that

$W = W(\Delta)$, and all possible W-equivariant lattices are given by the lattices $\mathcal{Q} \subseteq \mathcal{L} \subseteq \mathcal{P}$, where $\mathcal{Q}$ and $\mathcal{P}$ are the root and weight lattices of Δ, respectively. In particular, we note that $\mathcal{Q} \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{E}$ forces $\mathcal{L} \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{E}$.

We begin by observing that all lattices $\mathcal{Q} \subseteq \mathcal{L} \subseteq \mathcal{P}$ are automatically W-equivariant.

Lemma *Given an essential crystallographic root system Δ with root lattice $\mathcal{Q}$ and weight lattice P, then every lattice $\mathcal{Q} \subseteq \mathcal{L} \subseteq \mathcal{P}$ is W- (Δ-) equivariant.*

Proof It suffices to show that each element of W acts as the identity on $\mathcal{P}/\mathcal{Q}$. Moreover, since the group W is generated by reflections, we can reduce to looking at the reflections of W. Pick $x \in \mathcal{P}$. For any reflection $s_\alpha \in W$ and any $x \in \mathcal{P}$, we have

$$s_\alpha \cdot x = x - \langle \alpha, x \rangle \alpha.$$

Since $x \in \mathcal{P}$, we know, by definition, that $\langle \alpha, x \rangle \in \mathbb{Z}$. Thus $\langle \alpha, x \rangle \alpha \in \mathcal{Q}$ and $s_\alpha \cdot x \equiv x \pmod{\mathcal{Q}}$. ∎

We now prove the main result classifying crystallographic root systems.

Proposition *Let $W \subset O(\mathbb{E})$ be a finite essential reflection group, and let $\mathcal{L}$ be a W-equivariant lattice, where $\mathcal{L} \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{E}$. Then there is an essential crystallographic root system $\Delta \subset \mathcal{L}$, where:*

(i) $W = W(\Delta)$
(ii) $\mathcal{Q} \subseteq \mathcal{L} \subseteq \mathcal{P}$, where $\mathcal{P}$ and $\mathcal{Q}$ are the weight and root lattices of Δ.

Our argument is based on that of Farkas [1]. First of all, we need to locate the set $\Delta \subset \mathcal{L}$. For each reflection $s \in W$, let $\mathcal{L}_s \subset \mathcal{L}$ be defined by

$$\mathcal{L}_s = \{x \mid s \cdot x = -x\}.$$

The only two choices for $\mathcal{L}_s$ are $\mathcal{L}_s = 0$ or $\mathcal{L}_s = \mathbb{Z}$. We must have

$$\mathcal{L}_s = \mathbb{Z}.$$

It suffices to show $\mathcal{L}_s \neq 0$. Since $s(s-1) = 1 - s = -(s-1)$, we have $\operatorname{Im}(s-1) \subset \{x \mid s \cdot x = -x\}$; so it suffices to verify that $\operatorname{Im}(s-1) \neq 0$. Pick $x \in \mathcal{L}$ so that $s \cdot x \neq x$ (the inclusion $W \subset O(\mathbb{E})$ implies that each element of W acts nontrivially on $\mathbb{E}$. Since $\mathcal{L} \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{E}$, each element of W also acts nontrivially on $\mathcal{L}$). Then $y = s \cdot x - x \neq 0$.

Notice also, for future reference, that

$$\mathcal{L}_s \text{ is a direct summand of } \mathcal{L}.$$

Equivalently, $\mathcal{L}/\mathcal{L}_s$ is torsion free, i.e., if $nx \in \mathcal{L}_s$, then $x \in \mathcal{L}_s$ as well.

Finally, we choose the set

$$\Delta = \{\pm\alpha_s \mid s \in W \text{ is a reflection}\},$$

where $\pm\alpha_s$ are the two generators of $\mathcal{L}_s = \mathbb{Z}$ for the reflection $s \in W$.

Lemma A *The collection $\Delta = \{\pm\alpha_s\}$ is an essential crystallographic root system.*

Proof We need to verify four properties.

(B-1) Given $\alpha \in \Delta$, then $\lambda\alpha \in \Delta$ if and only if $\lambda = \pm 1$.

This property follows from the construction of Δ.

(B-2) Δ is invariant under W.

Pick $\alpha \in \Delta$ and $\varphi \in W$. We have $\alpha \in \mathcal{L}_s$ for some reflection $s \in W$. Since s is a reflection, it follows from property (A-4) of §1-1 that $\varphi s \varphi^{-1}$ is also a reflection. Next, φ induces an isomorphism

$$\varphi\colon \mathcal{L}_s \cong \mathcal{L}_{\varphi s \varphi^{-1}}.$$

To establish this fact, observe that the isomorphism $\varphi\colon \mathcal{L} \to \mathcal{L}$ induces a map $\varphi\colon \mathcal{L}_s \to \mathcal{L}_{\varphi s\varphi^{-1}}$. For given $x \in \mathcal{L}_s$, then $\varphi \cdot \alpha$ satisfies $(\varphi s \varphi^{-1})(\varphi \cdot x) = -\varphi \cdot x$ so that $\varphi \cdot x$ is an element of $\mathcal{L}_{\varphi s\varphi^{-1}}$. Conversely, the isomorphism $\varphi^{-1}\colon \mathcal{L} \to \mathcal{L}$ induces the inverse map $\varphi^{-1}\colon \mathcal{L}_{\varphi s\varphi^{-1}} \to \mathcal{L}_s$.

Finally, since α is a generator of $\mathcal{L}_s = \mathbb{Z}$, it follows that $\varphi \cdot \alpha$ must be one of the generators of $\mathcal{L}_{\varphi s\varphi^{-1}}$. So $\varphi \cdot \alpha \in \Delta$.

(B-3) Δ is crystallographic.

Given $\alpha, \beta \in \Delta$, then, by property (B-2), $\beta - \langle \alpha, \beta \rangle \alpha = s_\alpha \cdot \beta \in \mathcal{L}$. Since $\beta \in \mathcal{L}$, we must have $\langle \alpha, \beta \rangle \alpha \in \mathcal{L}$. Since α generates the direct summand $\mathcal{L}_s = \mathbb{Z}$ of $\mathcal{L}$, this is only possible if $\langle \alpha, \beta \rangle \in \mathbb{Z}$.

(B-4) Δ is essential.

Since $W \subset O(\mathbb{E})$ is an essential reflection group, we know that any associated root system is essential. ■

Having constructed Δ, we want to show that:

Lemma B *$\mathcal{Q} \subseteq \mathcal{L} \subseteq \mathcal{P}$, where $\mathcal{P}$ and $\mathcal{Q}$ are the weight and root lattices of Δ.*

Proof Since $\Delta \subset \mathcal{L}$, we have $\mathcal{Q} \subseteq \mathcal{L}$. As regards $\mathcal{L} \subset \mathcal{P}$, we use an argument similar to that used above to prove property (B-3). Given $\alpha \in \Delta$ and $x \in \mathcal{L}$, we want to show $\langle \alpha, x \rangle \in \mathbb{Z}$. $\mathcal{L}$ being invariant under W implies

$$x - \langle \alpha, x \rangle \alpha = s_\alpha \cdot x \in \mathcal{L}.$$

By arguing as in the (B-3) case of the previous lemma, we can now show that is only possible if $\langle \alpha, \beta \rangle \in \mathbb{Z}$. ■

This completes the proof of the above proposition. The only question left to deal with is the uniqueness of the root system $\Delta \subset \mathcal{L}$ chosen above. We shall do this in §10-1. There we shall define what it means for two root systems to be isomorphic. Given a W-equivariant isomorphism $\varphi\colon \mathcal{L} \cong \mathcal{L}'$, then φ will turn out to induce an isomorphism $\Delta \cong \Delta'$ of the root systems $\Delta \subset \mathcal{L}$ and $\Delta' \subset \mathcal{L}'$ chosen as above.

Remark: We close this chapter with another observation regarding the definition of reducibility as given in §9-1. We defined a Weyl group W to be reducible if it can be decomposed $W = W_1 \times W_2$ as a reflection group. We now see that both W_1 and W_2 in any such reflection group decomposition must be Weyl groups. This follows from the just-established fact that the Weyl group $W \subset O(\mathbb{E})$ has a crystallographic root system. As explained in Lemma 2-1, if $W = W(\Delta)$, then there is an orthogonal decomposition $\Delta = \Delta_1 \coprod \Delta_2$, where $W_1 = W(\Delta_1)$ and $W_2 = W(\Delta_2)$. If Δ is crystallographic, then Δ_1 and Δ_2 must be as well. Hence, W_1 and W_2 are Weyl groups.

10 The Classification of crystallographic root systems

In this chapter we classify crystallographic root systems. In view of the discussion in §9-5, we shall then have also achieved a classification of Weyl groups. As we have already mentioned in the introduction to Part III, the study of Weyl groups and crystallographic root systems uses the results about reflection groups from Chapters 1 through 8. In particular, the classification of Weyl groups and crystallographic root systems will turn out to be refinements of the classification of reflection groups obtained in Chapter 8.

10-1 Isomorphism of root systems

The purpose of this chapter is to classify essential crystallographic root systems up to an appropriately defined version of isomorphism. In this first section, we introduce and discuss the version of "isomorphism" to be used for root systems. In Chapter 9, we established a relationship between crystallographic root systems and Weyl groups. The definition of isomorphism for root systems is designed to be compatible, under this relation, with the already-defined concept of isomorphism for Weyl groups (see §9-1). We shall comment further on this connection at the end of the section.

We continue to use the very convenient notation

$$\langle \alpha, \beta \rangle = \frac{2(\alpha, \beta)}{(\alpha, \alpha)}.$$

We recall, in particular, that we can rewrite our standard formula for the reflection s_α as

$$s_\alpha \cdot x = x - \langle \alpha, x \rangle \alpha.$$

Definition: Two root systems $\Delta \subset \mathbb{E}$ and $\Delta' \subset \mathbb{E}'$ are *isomorphic* if there exists a linear isomorphism $f \colon \mathbb{E} \to \mathbb{E}'$, where

(i) $f(\Delta) = \Delta'$;
(ii) $\langle f(\alpha), f(\beta) \rangle = \langle \alpha, \beta \rangle$ for all $\alpha, \beta \in \Delta$.

Our definition of isomorphism for root systems is the one that has to be used if it is to fit into the discussion of §9-5. In particular, it is designed to enable us to reduce the classification of essential Weyl groups (up to isomorphism) to that of classifying essential crystallographic root systems (up to isomorphism).

Condition (ii) of the definition has various reformulations. The rest of this section will establish and discuss these reformulations.

Proposition *Given essential root systems $\Delta \subset \mathbb{E}$ and $\Delta' \subset \mathbb{E}'$ and a linear map $f \colon \mathbb{E} \to \mathbb{E}'$ such that $f(\Delta) = \Delta'$ then the following are equivalent:*

(i) $\langle f(\alpha), f(\beta) \rangle = \langle \alpha, \beta \rangle$ *for all* $\alpha, \beta \in \Delta$.

(ii) For all $\alpha \in \Delta$, we have a commutative diagram:

$$\begin{array}{ccc} \mathbb{E} & \xrightarrow{f} & \mathbb{E}' \\ {\scriptstyle s_\alpha}\downarrow & & \downarrow{\scriptstyle s_{f(\alpha)}} \\ \mathbb{E} & \xrightarrow{f} & \mathbb{E}' \end{array}$$

(iii) f preserves the angles θ between vectors and the ratio of lengths $\frac{\|\alpha\|}{\|\beta\|}$ for all elements $\alpha, \beta \in \Delta$.

Proof We begin with the equivalence of (i) and (ii). Fix $\alpha \in \Delta$ and consider the diagram in (ii). First of all,

$(*)$ the diagram commutes for all $x \in \mathbb{E} \Longleftrightarrow$ it commutes for all $\beta \in \Delta$.

This equivalence follows from the fact that Δ spans $\mathbb{E}$. Secondly,

$(**)$ the diagram commutes for $\beta \in \Delta \Longleftrightarrow \langle f(\alpha), f(\beta)\rangle = \langle \alpha, \beta\rangle$.

This equivalence is based on the identities

$$f(s_\alpha \cdot \beta) = f(\beta - \langle \alpha, \beta\rangle\alpha) = f(\beta) - \langle \alpha, \beta\rangle f(\alpha)$$
$$s_{f(\alpha)} f(\beta) = f(\beta) - \langle f(\alpha), f(\beta)\rangle f(\alpha).$$

It follows from $(*)$ and $(**)$ that conditions (i) and (iii) are equivalent.

Next, we consider the equivalence of (i) and (iii). The identity

$$(\alpha, \beta) = \|\alpha\|\,\|\beta\| \cos\theta$$

gives rise to the identities

(D-1) $\langle \alpha, \beta\rangle = \frac{2(\alpha,\beta)}{(\alpha,\alpha)} = 2\frac{\|\alpha\|\,\|\beta\|}{\|\alpha\|\,\|\alpha\|}\cos\theta = 2\frac{\|\beta\|}{\|\alpha\|}\cos\theta$
(D-2) $\langle \alpha, \beta\rangle\langle \beta, \alpha\rangle = 4\cos^2\theta$.

It follows from (D-1) that condition (iii) implies condition (i). The fact that condition (i) implies condition (iii) demands some argument. Suppose $\langle f(\alpha), f(\beta)\rangle = \langle \alpha, \beta\rangle$ for all $\alpha, \beta \in \Delta$. First of all, f preserves angles. Let θ (respectively, $\hat{\theta}$) be the angle between α and β (respectively, $f(\alpha)$ and $f(\beta)$). Property (D-2) implies that $\cos\theta = \pm\cos\hat{\theta}$. Property (D-1) then implies that $\cos\theta = \cos\hat{\theta}$. Finally, since $0 \le \theta, \hat{\theta} \le \pi$, $\cos\theta = \cos\hat{\theta}$ implies $\theta = \hat{\theta}$.

Secondly, f preserves ratio of lengths. To prove this, use (D-1) and the above fact that $\cos\theta = \cos\hat{\theta}$. ■

Remark: Condition (iii) of the above proposition is the key to classifying crystallographic root systems. It demonstrates that isomorphisms of root systems reduce

to specific geometric (indeed, trigonometric) information about the root systems. This geometric information imposes significant restrictions on the possibilities for crystallographic root systems. The study of the angles between root vectors and the ratios of their lengths will play an important part in the classification arguments of §10-3, §10-4 and §10-5.

It follows that we can reduce the classification of essential Weyl groups (up to isomorphism) to that of essential crystallographic root systems (up to isomorphism). As in Chapter 9 we shall approach Weyl groups in terms of equivariant lattices.

First of all, it was demonstrated in §9-5 that each crystallographic root system Δ gives rise to a number of W- (Δ-) equivariant lattices $\mathcal{Q} \subset \mathcal{L} \subset \mathcal{P}$. It is easy to see that isomorphic root systems, where "isomorphism" is defined as above, must give rise to isomorphic collections of equivariant lattices.

Conversely, it was demonstrated in §9-5 that every Weyl group must arise from a crystallographic root system in the above fashion, and it is now also easy to see that isomorphic Weyl groups must arise from isomorphic root systems. Given a Weyl group $W \subset O(\mathbb{E})$ with equivariant lattice $\mathcal{L}$, we locate a crystallographic root system $\Delta \subset \mathcal{L}$ by choosing, for each reflection s, the two generators $\pm\alpha_s$ of the subspace $\mathrm{Im}(s-1) = \mathbb{Z}$ and then letting $\Delta = \{\pm\alpha_s\}$. Suppose that $\mathcal{L}$ and $\mathcal{L}'$ are two equivariant lattices for the reflection group $W \subset O(\mathbb{E})$, and that $f\colon \mathcal{L} \to \mathcal{L}'$ is a W-equivariant linear isomorphism. Given $s \in W$, then the diagram

$$\begin{tikzcd} \mathcal{L} \arrow[r, "f"] \arrow[d, "s"] & \mathcal{L}' \arrow[d, "s'"] \\ \mathcal{L} \arrow[r, "f"] & \mathcal{L}' \end{tikzcd}$$

commutes, where s' denotes s when it acts on $\mathcal{L}'$. Since f is an isomorphism, it induces an isomorphism $\mathrm{Im}(s-1) \cong \mathrm{Im}(s'-1)$. In particular, if s is a reflection and $\pm\alpha$ are the generators of $\mathrm{Im}(s-1) = \mathbb{Z}$, then s' is a reflection and $\pm f(\alpha)$ are the generators of $\mathrm{Im}(s'-1) = \mathbb{Z}$. It is now easy to deduce that $f(\Delta) = \Delta'$, and that property (b) of the above proposition holds. Consequently, f satisfies both properties required for a root system isomorphism.

10-2 Cartan matrices

We shall demonstrate in this section that, to determine the isomorphism class of an essential crystallographic root system, we can reduce to any of its fundamental systems. This reduction is carried out via the Cartan matrix. Let Δ be an essential crystallographic root system.

Definition: The *Cartan matrix* of Δ is the $\ell \times \ell$ matrix $[\langle \alpha_i, \alpha_j \rangle]_{\ell\times\ell}$, where $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$ is a fundamental system of Δ.

The Cartan matrix requires the choice of a fundamental system Σ and an ordering of that system. There is an indeterminacy in the Cartan matrix arising from

the order imposed on Σ. Namely, it is only well defined up to column and row permutations. Such permutations arise from altering the order of the elements in Σ. We shall identify any two matrices related by such permutations. The Cartan matrix is then independent of the choice of Σ because any two choices of a fundamental system are linked via an element $\varphi \in W(\Delta)$ and $\langle \varphi \cdot \alpha_i, \varphi \cdot \alpha_j \rangle = \langle \alpha_i, \alpha_j \rangle$ for each $1 \leq i, j \leq \ell$. The rest of this section will be devoted to proving:

Theorem *The Cartan matrix of Δ determines Δ up to isomorphism.*

To prove the proposition, suppose we are given root systems

$$\Delta \subset \mathbb{E} \quad \text{and} \quad \Delta' \subset \mathbb{E}'$$

with fundamental systems

$$\Sigma = \{\alpha_1, \ldots, \alpha_\ell\} \quad \text{and} \quad \Sigma' = \{\alpha'_1, \ldots, \alpha'_\ell\}$$

such that

$$\langle \alpha_i, \alpha_j \rangle = \langle \alpha'_i, \alpha'_j \rangle \quad \text{for all } 1 \leq i, j \leq \ell.$$

We can define the obvious linear isomorphism f

$$f\colon \mathbb{E} \to \mathbb{E}'$$
$$f(\alpha_i) = \alpha'_i.$$

To prove the proposition, we must show:

(i) $f(\Delta) = \Delta'$;
(ii) $\langle \alpha, \beta \rangle = \langle f(\alpha), f(\beta) \rangle$ for all $\alpha, \beta \in \Delta$.

The rest of this section is devoted to the proof of these two facts. Observe that we don't know whether f preserves inner products; otherwise (ii) would be trivial. First of all, we have

(a) $f s_{\alpha_i} f^{-1} = s_{\alpha'_i}$ for $1 \leq i \leq \ell$.

Because of linearity in the second factor, the identities $\langle \alpha_i, \alpha_j \rangle = \langle \alpha'_i, \alpha'_j \rangle$ for $1 \leq i, j \leq \ell$ tell us that, for all $x \in \mathbb{E}$, we have the identity

$$\langle \alpha_i, x \rangle = \langle \alpha'_i, f(x) \rangle \quad \text{for } 1 \leq i \leq \ell.$$

It follows that the diagram

$$\begin{tikzcd} \mathbb{E} \arrow[r, "f"] \arrow[d, "s_{\alpha_i}"'] & \mathbb{E}' \arrow[d, "s_{\alpha'_i}"] \\ \mathbb{E} \arrow[r, "f"] & \mathbb{E}' \end{tikzcd}$$

commutes for $i = 1, \ldots, \ell$. (We use the fact that $s_{\alpha_i} \cdot x = x - \langle \alpha_i, x \rangle \alpha_i$.)

We can extend (a) to the assertion

(b) The map $\varphi \mapsto f\varphi f^{-1}$ induces an isomorphism $W(\Delta) \cong W(\Delta')$.

This follows from (a), and from the fact that $\{s_{\alpha_i}\}$ generates $W(\Delta)$ and $\{s_{\alpha_i'}\}$ generates $W(\Delta')$.

We now turn to the proof of the conditions (i) and (ii).

Proof of (i) First of all, $f(\Delta) \subset \Delta'$. Choose $\alpha \in \Delta$. Using Proposition 3-6, choose $\alpha_i \in \Sigma$ and $\varphi \in W(\Delta)$ such that

$$\varphi \cdot \alpha_i = \alpha.$$

Let $\varphi' = f\varphi f^{-1}$. By (b), $\varphi' \in W(\Delta')$. And we have

$$f(\alpha) = f(\varphi \cdot \alpha_i) = \varphi' \cdot f(\alpha_i) = \varphi' \cdot \alpha_i'.$$

Thus $f(\alpha) \in \Delta'$.

Secondly, f maps Δ onto Δ'. For pick $\alpha' \in \Delta'$. Using Proposition 3-6, choose $\alpha_i' \in \Sigma'$ and $\varphi' \in W(\Delta')$ such that

$$\varphi' \cdot \alpha_i' = \alpha'.$$

Next, choose $\alpha_i \in \Sigma$ and $\varphi \in W(\Delta)$, where

$$f(\alpha_i) = \alpha_i'$$

$$f\varphi f^{-1} = \varphi'.$$

This last property can also be written $f\varphi = \varphi' f$. If we let $\alpha = \varphi \cdot \alpha_i$, we must have

$$f(\alpha) = f(\varphi \cdot \alpha_i) = \varphi' \cdot f(\alpha_i) = \varphi' \cdot \alpha_i' = \alpha'.$$

Proof of (ii) We begin by showing that, given $\alpha \in \Delta$, we have, in $W(\Delta')$, the identity

$$(*) \qquad f s_\alpha f^{-1} = s_{f(\alpha)}.$$

If we choose $\alpha_i \in \Sigma$ and $\varphi \in W(\Delta)$ such that $\varphi \cdot \alpha_i = \alpha$, then, by property (A-4) of §1-1, we also have

$$\varphi s_{\alpha_i} \varphi^{-1} = s_\alpha.$$

Let $\varphi' = f\varphi f^{-1} \in W(\Delta')$ and let $\alpha_i' = f(\alpha_i)$. Then we have

$$f s_\alpha f^{-1} = f\varphi s_{\alpha_i} \varphi^{-1} f^{-1} = \varphi' f s_{\alpha_i} f^{-1} \varphi'^{-1} = \varphi' s_{\alpha_i'} \varphi'^{-1} = s_{\varphi' \cdot \alpha_i'}.$$

Notably, the second-to-last identity follows from part (a) above, whereas the last identity is property (A-4) of §1-1.

Identity $(*)$ now follows; for the sequence of identities appearing at the end of the proof of (i) imply that

$$f(\alpha) = \varphi' \cdot \alpha_i'.$$

Given $x \in \mathbb{E}$, if we apply the two sides of $(*)$ to $f(x)$, we obtain

$$\text{LHS} = (f s_\alpha f^{-1}) f(x) = f(x - \langle \alpha, x \rangle \alpha) = f(x) - \langle \alpha, x \rangle f(\alpha)$$

$$\text{RHS} = s_{f(\alpha)} f(x) = f(x) - \langle f(\alpha), f(x) \rangle f(\alpha).$$

So $\langle \alpha, x \rangle = \langle f(\alpha), f(x) \rangle$ for all $x \in \mathbb{E}$.

$\langle\alpha,\beta\rangle$	$\langle\beta,\alpha\rangle$	$\theta_{\alpha\beta}$	$\|\alpha\|^2/\|\beta\|^2$
0	0	$\pi/2$	?
1	1	$\pi/3$	1
-1	-1	$2\pi/3$	1
1	2	$\pi/4$	2
-1	-2	$3\pi/4$	2
1	3	$\pi/6$	3
-1	-3	$5\pi/6$	3

Table 1: Relations for arbitrary roots

10-3 Angles and ratios of lengths

By the results of §10-2, in order to classify essential crystallographic root systems up to isomorphism, we have to look at the integers $\langle\alpha_i,\alpha_j\rangle$, where $\{\alpha_1,\ldots,\alpha_\ell\}$ is a fundamental system of the root system. In §10-1, we obtained the identity

(D-1) $$\langle\alpha,\beta\rangle = 2\frac{\|\beta\|}{\|\alpha\|}\cos\theta_{\alpha,\beta},$$

where $\theta_{\alpha,\beta}$ is the angle between α and β. So the integer $\langle\alpha_i,\alpha_j\rangle$ is actually determined by the possible angles between the vectors, as well as by the ratio of their lengths.

We now set about studying angles and ratios of length. Before concentrating on fundamental roots, we first consider arbitrary root vectors $\alpha,\beta\in\Delta$. As in §10-1, we can use (D-1) to deduce the following identity

(D-2) $$\langle\alpha,\beta\rangle\langle\beta,\alpha\rangle = 4\cos^2\theta_{\alpha\beta},$$

where $\theta_{\alpha\beta}$ is the angle between α and β. Since $\langle\alpha,\beta\rangle\in\mathbb{Z}$ and $\langle\beta,\alpha\rangle\in\mathbb{Z}$, we conclude from (D-2) that

$$\langle\alpha,\beta\rangle\langle\beta,\alpha\rangle = 0,1,2,3,4$$

are the only possibilities.

Case $\langle\alpha,\beta\rangle\langle\beta,\alpha\rangle = 4$ This case is the degenerate case. By property (D-2), we must have $\cos\theta_{\alpha\beta} = \mp 1$. Thus by property (D-1), $\theta_{\alpha\beta} = 0$ or π and $\alpha = \mp\beta$.

Case $\langle\alpha,\beta\rangle\langle\beta,\alpha\rangle = 0,1,2,3$ These are the cases where $\alpha\neq\mp\beta$. Table 1 lists all possibilities. We assume $\|\alpha\|\geq\|\beta\|$. Observe that it follows from property (D-1) that $|\langle\alpha,\beta\rangle|\leq|\langle\beta,\alpha\rangle|$.

If we now assume that α and β are fundamental roots, then the possibilities for α and β are even further restricted. We have Table 2.

For, as deduced in Lemma 3-3B, we must have $(\alpha,\beta)\leq 0$ and $(\beta,\alpha)\leq 0$ if $\alpha\neq\beta\in\Sigma$. Consequently, $\langle\alpha,\beta\rangle<0$ and $\langle\beta,\alpha\rangle<0$ as well.

$\langle\alpha,\beta\rangle$	$\langle\beta,\alpha\rangle$	$\theta_{\alpha\beta}$	$\|\alpha\|^2/\|\beta\|^2$
0	0	$\pi/2$	?
-1	-1	$2\pi/3$	1
-1	-2	$3\pi/4$	2
-1	-3	$5\pi/6$	3

Table 2: Relations for fundamental roots

10-4 Coxeter graphs and Dynkin diagrams

In order to determine Δ up to isomorphism, we have to study the integers $\{\langle\alpha,\beta\rangle\}$, where $\alpha,\beta\in\Sigma$. In turn, identity (D-1) of §10-3 shows that it suffices to study the angles $\{\theta_{\alpha\beta}\}$ as well as the ratios $\{\|\alpha\|^2/\|\beta\|^2\}$. This turns out to be highly efficient because we can use a modification of the Coxeter graph to describe these data. This modification is called a Dynkin diagram. In the case of Coxeter graphs, we are working over $\mathbb{R}$ and codifying structural information about reflection groups. In the case of Dynkin diagrams, we are working over $\mathbb{Z}$ and codifying information about Weyl groups.

(A) The Coxeter Graph As explained in §8-7, Coxeter graphs codify information about the angles $\theta_{\alpha\beta}$. In preparation for the introduction of Dynkin diagrams, we shall alter the notation for Coxeter graphs, using extra edges between vertices, rather than labelling edges with integers. We assign a graph X to Δ by the rule

(i) $\Sigma=$ the vertices of X;
(ii) Given $\alpha\neq\beta\in\Sigma$ we assign $0,1,2$ or 3 edges between α and β by the following rule:

0 0	$\theta=\pi/2$
0$-$0	$\theta=2\pi/3$
0$=$0	$\theta=3\pi/4$
0$\equiv$0	$\theta=5\pi/6$

This is equivalent to the Coxeter graph of Δ described in §8-7. To translate, replace 0$-$0, 0$=$0, 0$\equiv$0 by the labelled edges $0\overset{3}{-}0$, $0\overset{4}{-}0$ and $0\overset{6}{-}0$. As before, the graph is connected if and only if Δ is irreducible.

(B) The Dynkin Diagram We also want to keep track of the ratio $\|\alpha\|/\|\beta\|$ of root lengths. The following lemma suggests that this problem of keeping track of root lengths is relatively simple to handle.

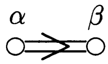
Lemma *If Δ is irreducible, then at most two root lengths occur in Δ.*

Proof By Theorem 3-6, it suffices to prove that at most two root lengths occur in Σ. Consider the Coxeter graph of Δ. If there is a single edge between two vertices $\alpha,\beta\in\Sigma$, then, by Table 2 at the end of §10-3, α and β have the same length. But,

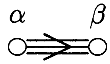
by the classification result given in §8-1, we have, with one possible exception, either a single edge or no edge between any two vertices. Also, the Coxeter graph is connected. These facts restrict the root lengths as desired. ■

In the case where two root lengths occur, we call the roots *short* and *long*. We might note that all the root vectors of the same length lie in the same $W(\Delta)$ orbit. So Δ divides into, at most, two $W(\Delta)$ orbits.

Given fundamental roots of different length, we can use arrows in the Coxeter diagram to clarify the relation between their lengths. Namely, in the case of a double or triple edge between two roots (= vertices), we add an arrow pointing towards the shorter root. So if $\|\alpha\| > \|\beta\|$, we have



or



These arrows introduced into the Coxeter graph serve to distinguish the shorter and longer roots. A Coxeter graph with such arrows is called a *Dynkin diagram.*

10-5 The classification of root systems

We now have a program for classifying irreducible essential crystallographic root systems.

(a) Draw up a list of possible Coxeter graphs for irreducible essential crystallographic root systems. This list is achieved by going through the classification result of §8-7 and picking out all Coxeter graphs where the edges are labelled by 3, 4 or 6. This results in the elimination of H_3, H_4 and $G_2(m)$ except for $G_2 = G_2(6)$.

(b) For each Coxeter graph chosen in (a), determine all distinct ways of forming a Dynkin diagram, i.e., of introducing arrows into the Coxeter diagram. In only one case, that of the B_ℓ graph, can we introduce arrows in two distinct ways.

(c) Finally, show that all the possibilities obtained in (b) can be realized by crystallographic root systems.

Steps (a) and (b) lead to the following list of possibilities.

Theorem A *If Δ is an irreducible essential crystallographic root system, then its Dynkin diagram must be in Table 3.*

To complete step (c) of the classification program, we also have to show:

Theorem B *There exists a crystallographic root system having each of A_ℓ, B_ℓ, ..., F_4, G_2 as its Dynkin diagram.*

But this follows from our previous work. Root systems for all of A_ℓ, B_ℓ, ..., F_4, G_2 except for C_ℓ were given in §8-7. The root system C_ℓ was defined in §2-2. The fact that each of these root systems is crystallographic can easily be verified.

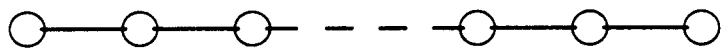
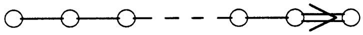
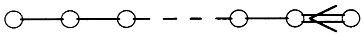
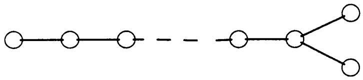
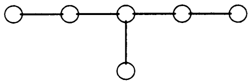
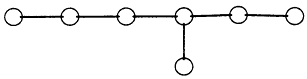
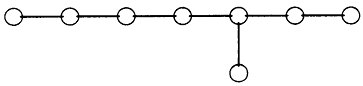
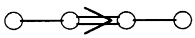
(A_ℓ)		$(\ell \geq 1)$
(B_ℓ)		$(\ell \geq 2)$
(C_ℓ)		$(\ell \geq 2)$
(D_ℓ)		$(\ell \geq 4)$
(E_6)		
(E_7)		
(E_8)		
(F_4)		
(G_2)		

Table 3: Dynkin diagrams of essential crystallographic root systems

11 Affine Weyl groups

We can pass from the Weyl group of a crystallographic root system and form an infinite group that has more information about the root system, and yet still possesses a structure analogous to that of the Weyl group. Notably, it has a Coxeter group structure. This group is called the affine Weyl group. Affine Weyl groups have a number of uses. They will be used in Chapter 12 to analyze subroot systems of crystallographic root systems. They are even useful for understanding ordinary Weyl groups. This will be demonstrated in §11-6.

11-1 The affine Weyl group

Let Δ be a crystallographic root system. For each $\alpha \in \Delta$, we have defined the hyperplane

$$H_\alpha = \{t \in \mathbb{E} \mid (\alpha, t) = 0\}$$

and the associated reflection

$$s_\alpha \cdot x = x - \frac{2(\alpha, x)}{(\alpha, \alpha)}\alpha = x - (\alpha, x)\alpha^{v},$$

where α^{v} is the coroot

$$\alpha^{v} = \frac{2\alpha}{(\alpha, \alpha)}.$$

We now generalize these concepts. For each $k \in \mathbb{Z}$ and $\alpha \in \Delta$, we can define the hyperplane

$$H_{\alpha,k} = \{t \in \mathbb{E} \mid (\alpha, t) = k\}$$

and the reflection $s_{\alpha,k}$ in the hyperplane $H_{\alpha,k}$

$$s_{\alpha,k} \cdot x = x - (\alpha, x)\alpha^{v} + k\alpha^{v}.$$

Observe that the case $k = 0$ gives the hyperplane H_α and its associated reflection s_α as discussed above. By introducing these extra reflections, the ordinary Weyl group can be extended to the affine Weyl group. We define the *affine Weyl group* by

Definition: $W_{\text{aff}}(\Delta) =$ the group generated by $\{s \mid \alpha \in \Delta, k \in \mathbb{Z}\}$.

As we shall see in §11-3, $W_{\text{aff}} = W_{\text{aff}}(\Delta)$ is a Coxeter group. In the remainder of this section, we establish that W_{aff} has a semidirect product decomposition in terms of the Weyl group W and the coroot lattice $\mathcal{Q}^{v}$. (The coroot lattice was defined and discussed in §9-2. Here we shall be interpreting it as translations on $\mathbb{E}$.)

Proposition $W_{\text{aff}} = \mathcal{Q}^{v} \rtimes W$.

Proof We need to show:

(i) W and $\mathcal{Q}^\vee$ are subgroups of W_{aff};
(ii) $W_{\text{aff}} = \mathcal{Q}^\vee W$;
(iii) $\mathcal{Q}^\vee \cap W = \{0\}$;
(iv) $\mathcal{Q}^\vee$ is normal.

(i): We have already shown that $W \subset W_{\text{aff}}$. Regarding $\mathcal{Q}^\vee$, any $d \in \mathbb{E}$ defines a translation

$$T(d)\colon \mathbb{E} \to \mathbb{E}$$

$$T(d)(x) = x + d.$$

Moreover, $T(d)T(d') = T(d+d')$. Thus $\mathcal{Q}^\vee$ gives a group of translations on $\mathbb{E}$. We have the identity

$$(*) \qquad s_{\alpha,k} = T(k\alpha^\vee)s_\alpha$$

(check the effect of RHS on $H_{\alpha,k}$ and on 0). Thus for all $\alpha \in \Delta$ and $k \in \mathbb{Z}$, $T(k\alpha^\vee) = s_{\alpha,k}s_\alpha^{-1} \in W_{\text{aff}}$. In particular, $\{T(\alpha_1^\vee), \ldots, T(\alpha_\ell^\vee)\} \subset W_{\text{aff}}$. So $\mathcal{Q}^\vee \subset W_{\text{aff}}$.

(ii): This follows from the above identity $(*)$.

(iii): Any nonzero element of $\mathcal{Q}^\vee$ is an element of infinite order while W is a finite group.

(iv): For any $d \in \mathcal{Q}^\vee$ and any $\varphi \in W$, we have the identity

$$\varphi T(d)\varphi^{-1} = T(\varphi \cdot d). \qquad \blacksquare$$

The rest of this chapter will be devoted to demonstrating that W_{aff} satisfies a number of properties analogous to those holding for finite Euclidean reflection groups. We shall show that W_{aff} has a Coxeter group structure that is a natural extension of the Coxeter group structure of W obtained in Chapter 6. In the process, we shall also show that there are precise analogues of previous structure theorems concerning the action of W on root systems and Weyl chambers.

11-2 The highest root

Let $\Delta \subset \mathbb{E}$ be an irreducible crystallographic root system and $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$ a fundamental system of Δ. In this section, we shall explain how to choose the *highest root* α_0 of Δ with respect to Σ. *Highest* refers to a partial order we can define on $\mathbb{E}$. Let

$$\mathcal{Q} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_\ell$$

be the root lattice as defined in §9-2. Choose $\mathcal{Q}^+ \subset \mathcal{Q}$ by the rule

$$\mathcal{Q}^+ = \{x_1\alpha_1 + \cdots + x_\ell\alpha_\ell \mid x_i \geq 0 \text{ for all } i\}.$$

We can use $\mathfrak{Q}^+$ to define a partial order, as follows.

Definition: Given $x, y \in \mathbb{E}$, then $x > y$ if $x \neq y$ and $x - y \in \mathfrak{Q}^+$.

The highest root α_0 is characterized by the property that $\alpha_0 \geq \alpha$ for all $\alpha \in \Delta$. We want to show that, for each choice of a fundamental system Σ, such a root exists and is unique. As a preliminary to showing that such an α_0 exists, we first show:

Lemma *Given $\alpha, \beta \in \Delta$ where $\alpha \neq \beta$, then*

(i) $(\alpha, \beta) > 0$ *forces* $\alpha - \beta \in \Delta$;
(ii) $(\alpha, \beta) < 0$ *forces* $\alpha + \beta \in \Delta$.

Proof We provide a detailed proof of (i). First of all, $(\alpha, \beta) > 0$ implies $\langle \alpha, \beta \rangle > 0$. By Table 4 in §10-3, it then follows that either $\langle \alpha, \beta \rangle = 1$ or $\langle \beta, \alpha \rangle = 1$. If $\langle \beta, \alpha \rangle = 1$, then

$$\alpha - \beta = \alpha - \langle \beta, \alpha \rangle \beta = s_\beta \cdot \alpha \in \Delta.$$

If $\langle \alpha, \beta \rangle = 1$, then

$$\beta - \alpha = \beta - \langle \alpha, \beta \rangle \alpha = s_\alpha \cdot \beta \in \Delta.$$

But then $\alpha - \beta = -(\beta - \alpha) \in \Delta$ as well. (ii) is established by a similar argument. ∎

We now prove

Theorem *There exists a unique $\alpha_0 \in \Delta$ such that $\alpha_0 \geq \alpha$ for all $\alpha \in \Delta$.*

Proof The elements of Δ form a partially ordered set with respect to "$\leq$". We shall show that any two elements of Δ that are maximal are identical. Let $\alpha_0 \in \Delta$ be such a maximal element. It has two important properties.

(a) $(\alpha_0, \alpha_i) \geq 0$ for $1 \leq i \leq \ell$. Moreover, $(\alpha_0, \alpha_i) > 0$ for some i.
(b) If we write $\alpha_0 = \sum h_i \alpha_i$, then $h_i > 0$ for all i.

Proof of (a) The fact that $(\alpha_0, \alpha_i) \geq 0$ for all i follows from part (ii) of the above lemma, and the maximality of α_0. Moreover, since $(\alpha_0, \alpha_0) \neq 0$, and since α_0 can be expanded in terms of $\{\alpha_1, \ldots, \alpha_\ell\}$, it follows that $(\alpha_0, \alpha_i) \neq 0$ for some i. The first sentence of the proof then forces the stronger result that $(\alpha_0, \alpha_i) > 0$.

Proof of (b) We begin by observing that the maximality of α_0 forces

$$\alpha_0 \in \Delta^+.$$

For, given $\alpha \in \Delta^+$ and $\beta \in \Delta^-$, we always have $\alpha > \beta$. Hence, elements of Δ^- cannot be maximal elements. So we know that $\alpha_0 = \sum h_i\alpha_i$, where $h_i \geq 0$ for all i. Now decompose $\Sigma = \Sigma_1 \coprod \Sigma_2$, where

$$\Sigma_1 = \{\alpha_i \mid h_i > 0\}$$
$$\Sigma_2 = \{\alpha_i \mid h_i = 0\}.$$

We shall show that $\Sigma_2 \neq \varnothing$ produces a contradiction. Given $\alpha \in \Sigma_1$ and $\beta \in \Sigma_2$, we always have $(\alpha, \beta) \leq 0$ (see Lemma A of §3-3). Moreover, for some choice of α and β, we have $(\alpha, \beta) < 0$. (Otherwise, the elements of Σ_1 and Σ_2 would be orthogonal to each other and Δ would not be an irreducible root system.) For this choice of β, we have $(\alpha_0, \beta) < 0$. By our previous lemma, we then have $\alpha_0 + \beta \in \Delta$, which contradicts the maximality of α_0 with respect to $\leq$.

Now, suppose that α_0 and α_0' are elements of Δ that are both maximal in Δ with respect to the ordering $\leq$. We want to show $\alpha_0 = \alpha_0'$. By property (a) for α_0 and property (b) for α_0', we have

$$(\alpha_0, \alpha_0') > 0.$$

It now follows from part (i) of the previous lemma that either $\alpha_0 = \alpha_0'$ or $\alpha_0 - \alpha_0' \in \Delta$. To apply the lemma we need only observe that $\alpha_0 \neq \alpha_0'$ actually implies the stronger fact that $\alpha_0 \neq \pm\alpha_0'$. The point is that both α_0 and $\alpha_0' \in \Delta^+$. For, as observed above, elements of Δ^- cannot be maximal elements.

We can eliminate $\alpha_0 - \alpha_0' \in \Delta$. Otherwise, we must have either $\alpha_0 - \alpha_0' \in \Delta^+$ or $\alpha_0' - \alpha_0 \in \Delta^+$. But then either $\alpha_0 > \alpha_0'$ or $\alpha_0' > \alpha_0$, contradicting the maximality of either α_0' or α_0, respectively. ∎

A description of the highest root α_0 for the various irreducible crystallographic root systems is provided in Table 4. The table consists of the Dynkin diagrams from §10-5 with some added information. Namely, we assign an integer to each vertex. These integers are the coefficients of the corresponding fundamental roots $\{\alpha_1, \ldots, \alpha_\ell\}$ in the expansion $\alpha_0 = \sum h_i\alpha_i$.

Remark: The number $h(\alpha_0) = (\sum h_i) + 1$ is called the *Coxeter number* of W. The Coxeter number also appears in Chapter 29, where it is defined as the order of any "Coxeter element" of W. However, we shall not show the equivalence of these two definitions.

We close this section by showing that highest roots satisfy another maximal property.

Proposition $\|\alpha_0\| \geq \|\alpha\|$ *for all* $\alpha \in \Delta$.

Proof It suffices to show that $(\alpha_0, \alpha_0) \geq (\alpha, \alpha)$. Let

$$\overline{\mathcal{C}_o} = \{t \in \mathbb{E} \mid (\alpha_i, t) \geq 0 \text{ for } i = 1, \ldots, \ell\}$$
$$= \{t \in \mathbb{E} \mid (\alpha, t) \geq 0 \text{ for } \alpha \in \Omega^+\}$$

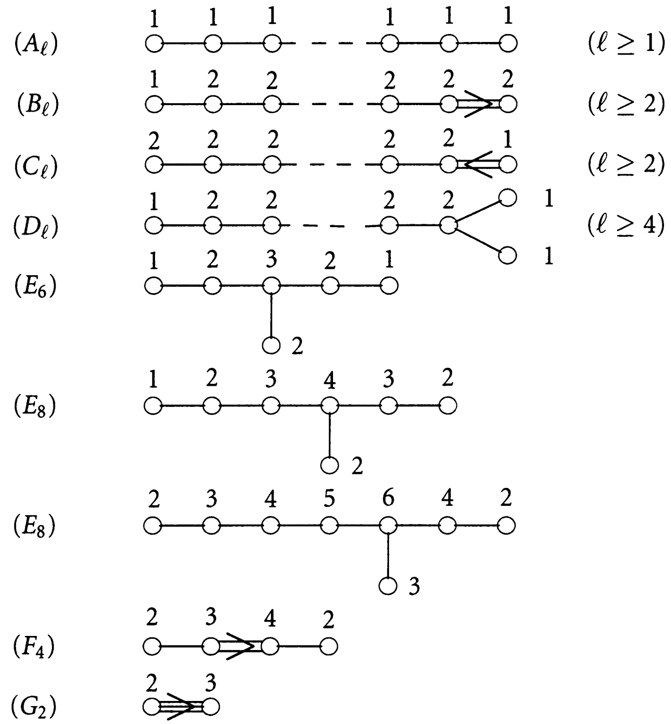


Table 4: Coefficients of highest roots

be the closure of the fundamental chamber (see §5-2). By fact (a) in the proof of the above theorem, we have

$$\alpha_0 \in \mathcal{C}_0.$$

Since $(\varphi \cdot \alpha, \varphi \cdot \alpha) = (\alpha, \alpha)$ for all $\varphi \in W$, we can replace α by $\varphi \cdot \alpha$ for any $\varphi \in W$. Since $\overline{\mathcal{C}_o}$ is a fundamental domain for the action of W on $\mathbb{E}$, we can therefore assume

$$\alpha \in \overline{\mathcal{C}_o}.$$

Since $\alpha_0 - \alpha \in \mathcal{Q}^+$, we have

$$(\alpha_0 - \alpha, t) \geq 0 \quad \text{for all } t \in \overline{\mathcal{C}_o}.$$

In particular, applying this inequality to $t = \alpha_0$ and $t = \alpha$, we obtain

$$(\alpha_0, \alpha_0) \geq (\alpha_0, \alpha) \geq (\alpha, \alpha).$$ ■

Remark: As observed in §10-4, there are actually only two root lengths in any irreducible crystallographic root systems. The proposition implies that a highest root is always a long root.

11-3 Affine Weyl groups as Coxeter groups

The next two sections are devoted to justifying that affine Weyl groups are Coxeter groups. In this section, we state the main result. The next section is concerned with details.

Let $\Delta \subset \mathbb{E}$ be a crystallographic root system. Let $W = W(\Delta)$ and $W_{\text{aff}} = W_{\text{aff}}(\Delta)$ be, respectively, the Weyl group and the affine Weyl group of Δ. In order to prove that W_{aff} is a Coxeter group, it suffices to deal with the case of an irreducible root system. For if

$$\Delta = \Delta_1 \coprod \cdots \coprod \Delta_k$$

is an orthogonal decomposition, then

$$W(\Delta) = W(\Delta_1) \times \cdots \times W(\Delta_k)$$
$$W_{\text{aff}}(\Delta) = W_{\text{aff}}(\Delta_1) \times \cdots \times W_{\text{aff}}(\Delta_k).$$

So we assume that Δ is irreducible as well.

Let $\Sigma = \{\alpha_1, \dots, \alpha_\ell\}$ be a fundamental system of Δ, and let α_0 be the highest root with respect to $\{\alpha_1, \dots, \alpha_\ell\}$. The Coxeter generators of W_{aff} will correspond to these roots. For each of the roots $\{\alpha_1, \dots, \alpha_\ell\}$, choose

$$s_i = s_{\alpha_i,0}, \text{ the reflection with respect to the hyperplane } H_{\alpha_i} = H_{\alpha_i,0}.$$

For α_0, choose

$$s_0 = s_{-\alpha_0,1}, \text{ the reflection with respect to the hyperplane } H_{-\alpha_0,1}.$$

For any $0 \le i, j \le \ell$, let

$$m_{ij} = \text{the order of } s_i s_j.$$

Theorem $W_{\text{aff}}(\Delta) = \langle s_0, s_1, \dots, s_\ell \mid (s_i s_j)^{m_{ij}} = 1 \rangle$.

The description of $W_{\text{aff}}(\Delta)$ given in the theorem is independent of the choice of the fundamental system $\Sigma = \{\alpha_1, \dots, \alpha_\ell\}$ because $W(\Delta)$ acts transitively on the set of fundamental systems of Δ. If Σ and Σ' are linked by $\varphi \in W(\Delta)$, then the inner automorphism $\varphi \_ \varphi^{-1} \colon W_{\text{aff}}(\Delta) \to W_{\text{aff}}(\Delta)$ provides an isomorphism between the two Coxeter descriptions of $W_{\text{aff}}(\Delta)$ provided by Σ and Σ'.

The Coxeter description of $W_{\text{aff}}(\Delta)$ is an extension of that for $W(\Delta)$ and is obtained by adjoining the extra reflection s_0. A similar pattern occurs when we turn to Coxeter graphs. The Coxeter system of each affine Weyl group $W_{\text{aff}}(\Delta)$ can be represented by a Coxeter graph, and this Coxeter graph is closely related to the Coxeter graph of the Weyl group $W(\Delta)$ as given in Chapter 6. In the irreducible case, we simply take the Coxeter graph of $W(\Delta)$ with vertices $\{s_1, \dots, s_\ell\}$, add an extra node corresponding to the extra reflection s_0, and determine the integers labelling the edges running from s_0 to $s_1, \dots, s_\ell$ by calculating the order of $s_0 s_i$ for

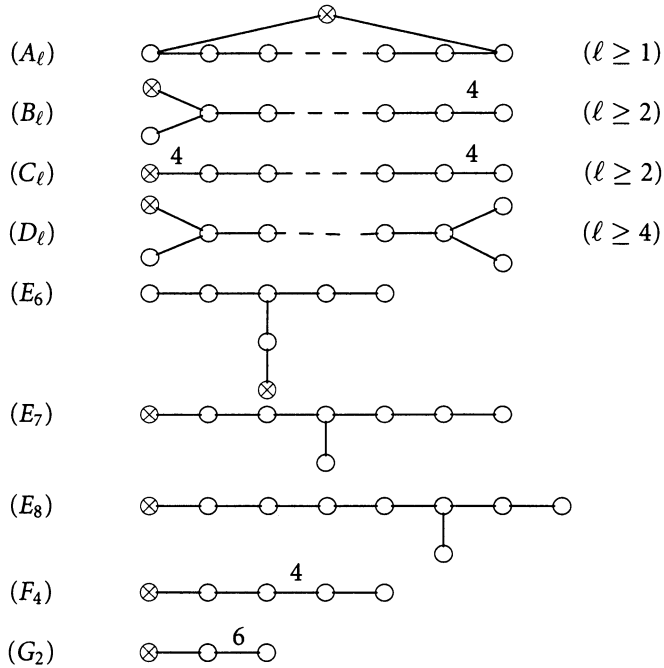


Table 5: Affine Coxeter graphs

$i = 1, \dots, \ell$. The Coxeter graphs of the affine Weyl groups for the root systems $A_\ell, B_\ell, \dots, G_2$ are displayed in Table 5.
We have indicated by "$\otimes$" the node corresponding to the reflection $s_{\alpha_0} = s_{-\alpha_0,1}$.

The proof of the above theorem is analogous to the proofs given in Chapters 4 and 6 demonstrating that finite reflection groups are Coxeter groups. We replace root systems by affine root systems and proceed as in Chapters 4 and 6. Using the action of W_{aff} on the affine root system, we show that W_{aff} is generated by $\{s_0, \dots, s_\ell\}$. Thus there is a concept of length in W_{aff} with respect to $\{s_0, \dots, s_\ell\}$ and, again using the action of W_{aff} on the affine root system, we show that length satisfies the Matsumoto exchange condition. Granted this condition, we prove the Coxeter property for W_{aff} as in §6-2.

The next two sections are devoted to the discussion of affine root systems and "alcoves", as well as further details about the proof of the theorem above. In closing, we might mention one more fact about the Coxeter structure of W_{aff}.

Remark: The finite Coxeter systems were characterized in Chapter 7 as those for which the associated bilinear form (see §7-1) is positive definite. The affine Coxeter systems can be characterized as those for which the associated bilinear form is *positive degenerate* (i.e., $\beta(x,x) \geq 0$ for all x, but $\beta(x,x) = 0$ for some $x \neq 0$).

11-4 Affine root systems

Affine Weyl groups have root systems associated with them. Throughout this section, we let $\Delta \subset \mathbb{E}$ be an irreducible crystallographic root system. The affine root system associated with Δ is the set

$$\Delta_{\text{aff}} = \Delta \times \mathbb{Z}.$$

We can think of $W_{\text{aff}}(\Delta)$ as the reflection groups associated with Δ_{aff} because we can associate hyperplanes, and hence reflections, to affine roots. Each $\lambda = (\alpha, k) \in \Delta_{\text{aff}}$ can be regarded as an affine function on $\mathbb{E}$

$$\lambda\colon \mathbb{E} \to \mathbb{R}$$
$$\lambda(x) = (\alpha, x) + k.$$

Given $\lambda = (\alpha, k)$, then

$$H_{\alpha,-k} = \operatorname{Ker} \lambda.$$

So we could designate $H_{\alpha,-k}$ and $s_{\alpha,-k}$ by H_λ and s_λ, respectively.

There is an action of W_{aff} on Δ_{aff} compatible with this correspondence. We want the action to satisfy the identities

$$\phi s_\lambda \phi^{-1} = s_{\phi\cdot\lambda}$$
$$\phi \cdot H_\lambda = H_{\phi\cdot\lambda}.$$

Given

$$\phi = T(d)s_\alpha \in W_{\text{aff}} = Q^\vee W$$

we have

$$\phi s_{\beta,k}\phi^{-1} = s_{s_\alpha\cdot\beta,k+(s_\alpha\cdot\beta,d)}$$

$$\phi\cdot H_{\beta,k} = H_{s_\alpha\cdot\beta,k+(s_\alpha\cdot\beta,d)}.$$

So we must define

$$\phi\cdot(\beta,k) = \big(s_\alpha\cdot\beta, k + (s_\alpha\cdot\beta,d)\big).$$

In particular, $s_\alpha\cdot(\beta,k) = (s_\alpha\cdot\beta,k)$.

(a) Fundamental Systems Given a fundamental system $\Sigma = \{\alpha_1,\ldots,\alpha_\ell\} \subset \Delta$, there is an associated fundamental system of Δ_{aff}. Let

$$\Sigma_{\text{aff}} = \{(\alpha_1,0),\ldots,(\alpha_\ell,0),(-\alpha_0,1)\},$$

where α_0 is the highest root of Δ with respect to Σ. We can decompose

$$\Delta_{\text{aff}} = \Delta_{\text{aff}}^+ \coprod \Delta_{\text{aff}}^-,$$

where

$$\Delta_{\text{aff}}^+ = \{(\alpha,n) \mid n \geq 1 \text{ or } n = 0 \text{ and } \alpha \in \Delta^+\}$$

$$\Delta_{\text{aff}}^- = \{(\alpha,n) \mid n \leq -1 \text{ or } n = 0 \text{ and } \alpha \in \Delta^-\}.$$

All the elements of Δ_{aff}^+ can be expanded in terms of Σ_{aff} with nonnegative coefficients, whereas the elements of Δ_{aff}^- can be expanded in terms of Σ_{aff} with nonpositive coefficients. (Hint: the coefficient of $(-\alpha_0,1)$ in the expansion of (α,n) is n.)

The Dynkin diagram of Δ can be extended to a larger diagram that represents Δ_{aff}. Table 6 gives the affine Dynkin diagram for all the irreducible crystallographic root systems. These affine diagrams will play an important role in Chapter 12.

(b) Height Analogously to §3-6, we can define the height of (α,n) with respect to Σ_{aff}. Height in Δ (with respect to Σ) and height in Δ_{aff} (with respect to Σ_{aff}) are related by

$$h(\alpha,n) = h(\alpha) + n[h(\alpha_0)+1].$$

In the rest of this section, we prove an analogue of the result on height obtained in §3-6. This is the one case where arguments in the affine case are substantially different from those in the finite case. Let $\{s_0,\ldots,s_\ell\}$ be the reflections defined in §11-3. (Observe that they are the reflections associated to the elements of Σ_{aff}.)

Proposition A *Let $W_0 \subset W_{\text{aff}}$ be the subgroup generated by $\{s_0,\ldots,s_\ell\}$. Given $\lambda \in \Delta_{\text{aff}}^+$, where $\lambda \notin \Sigma_{\text{aff}}$, then, for some $\varphi \in W_0$, we have:*

(A_ℓ) $(\ell \geq 1)$

(B_ℓ) $(\ell \geq 2)$

(C_ℓ) $(\ell \geq 2)$

(D_ℓ) $(\ell \geq 4)$

(E_6)

(E_7)

(E_8)

(F_4)

(G_2)

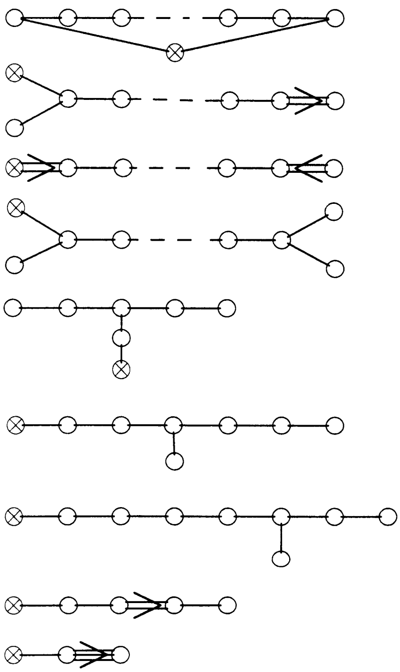


Table 6: Affine Dynkin diagrams

(i) $\varphi \cdot \lambda \in \Delta^+_{\text{aff}}$;
(ii) $h(\varphi \cdot \lambda) < h(\lambda)$.

Proof We have $W \subset W_0$. If $\lambda = (\alpha, 0)$, where $\alpha \in \Delta^+$, then, by Lemma 3-6, we can choose $\varphi \in W$ such that $\varphi \cdot \alpha \in \Delta^+$ and $h(\varphi \cdot \alpha) \leq h(\alpha)$. If $\lambda = (\alpha, k)$, where $\alpha \in \Delta$ and $k > 0$, we shall show that there exists $\varphi \in W_0$ such that $\varphi \cdot \lambda = (\beta, k-1)$ for some $\beta \in \Delta^+$. First of all,

$$(*) \qquad (\alpha_0, \varphi \cdot \alpha) \neq 0 \quad \text{for some } \varphi \in W,$$

because the W orbit of α generates a W stable subspace $V \subseteq \mathbb{E}$. The orthogonal complement of V is given by

$$V^\perp = \{x \in \mathbb{E} \mid (x, y) = 0 \text{ for all } y \in V\}.$$

It is also a W-stable subspace of $\mathbb{E}$. In order to prove $(*)$, it suffices to show

$$\alpha_0 \notin V^\perp.$$

This reduction follows from the irreducibility of Δ. For, given any $\beta \in \Delta$, we have $\beta \in V$ or $\beta \in V^\perp$. (Otherwise, the components of β in V and in $V^\perp$ would give independent elements on which s_β is multiplication by -1.) Consequently, we have a partition

$$\Delta = \Delta' \coprod \Delta'',$$

where both $\Delta' \subset V$ and $\Delta'' \subset V^\perp$ are root systems. Since $\alpha \in \Delta'$, we know that $\Delta' \neq \phi$. It follows that $\Delta'' = \phi$. Otherwise, we contradict the irreducibility of Δ. So $\Delta = \Delta' \subset V$. In particular, $\alpha_0 \in V$.

Choose φ as in $(*)$. By Proposition 11-2, $\|\alpha_0\| \geq \|\varphi \cdot \alpha\|$. By the chart in §10-3, we have $\langle \alpha_0, \varphi \cdot \alpha \rangle = \pm 1$. We can assume

$$\langle \alpha_0, \varphi \cdot \alpha \rangle = 1.$$

(If necessary, replace $\varphi \cdot \alpha$ by $(s_{\varphi \cdot \alpha} \varphi) \cdot \alpha = -\varphi \cdot \alpha$.) In view of identity $(*)$ in §11-1, and the fact that $s_{\alpha_0} = s_{-\alpha_0}$, we can write

$$s_0 = s_{-\alpha_0, 1} = T(-\alpha_0^\vee) s_{\alpha_0}.$$

If we use the action of W_{aff} on Δ_{aff} defined at the beginning of this section, we now have

$$\begin{aligned} s_0 \varphi \cdot (\alpha, k) &= s_0 \cdot (\varphi \cdot \alpha, k) = T(-\alpha_0^\vee) s_{\alpha_0} \cdot (\varphi \cdot \alpha, k) \\ &= \big(s_{\alpha_0} \varphi \cdot \alpha, k - (s_{\alpha_0} \varphi \cdot \alpha, \alpha_0^\vee)\big) = (s_{\alpha_0} \varphi \cdot \alpha, k - 1). \end{aligned}$$

For the last equality, we use the fact that

$$\begin{aligned}(s_{\alpha_0}\varphi \cdot \alpha, \alpha_0^\vee) &= (\alpha_0^\vee, s_{\alpha_0}\varphi \cdot \alpha) = \langle \alpha_0, s_{\alpha_0}\varphi \cdot \alpha\rangle \\ &= \langle s_{\alpha_0} \cdot \alpha_0, \varphi \cdot \alpha\rangle = \langle -\alpha_0, \varphi \cdot \alpha\rangle \\ &= -\langle \alpha_0, \varphi \cdot \alpha\rangle = -1.\end{aligned}$$

Lastly, by Corollary 3-6, every element of Δ is in the W orbit of a fundamental root. So if $(s_{\alpha_0}\varphi) \cdot \alpha \in \Delta^-$, we can find $\phi \in W$ such that $(\phi s_{\alpha_0}\varphi) \cdot \alpha \in \Delta^+$. ∎

The importance of this proposition is that it enables us to duplicate the arguments of §4-1, and to prove that W_{aff} is generated by the reflections $\{s_0, s_1, \dots, s_\ell\}$.

(c) Length As in §4-2, we can define length in W_{aff} with respect to $\{s_0, s_1, \dots, s_\ell\}$ and show that length can be characterized by:

Proposition B *$\ell(\varphi)$ = the number of positive roots converted by φ into negative roots.*

As a spinoff of these arguments, we also obtain the Matsumoto exchange property:

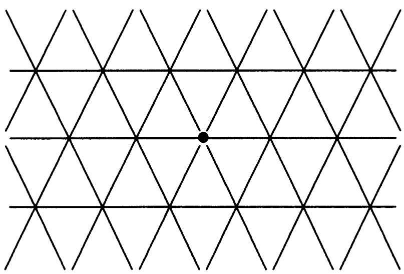
Proposition C *Given $\varphi = s_{k_1} \cdots s_{k_n}$, if $\ell(\varphi) < n$ then there exists $1 \le i < j < n$ such that*

$$s_{k_i} \cdots s_{k_j} = s_{k_{i+1}} \cdots s_{k_{j+1}}.$$

Granted this property, we can then prove the Coxeter property for W_{aff}, as in §6-2.

11-5 Alcoves

An *alcove* is a connected component of $\mathbb{E} - [\bigcup_{\substack{\alpha\in\Delta^+ \\ k\in Z}} H_{\alpha,k}]$. The following picture gives the alcove system of the root system A_2.



As this picture illustrates, the division into alcoves is a refinement of the division into chambers. Given a fundamental system $\Sigma = \{\alpha_1, \dots, \alpha_\ell\}$ and its corresponding highest root α_0, we can define the *fundamental alcove*

$$\begin{aligned}\mathcal{A}_0 &= \{t \in \mathbb{E} \mid 0 < (t, \alpha) < 1 \text{ for all } \alpha \in \Delta^+\} \\ &= \{t \in \mathbb{E} \mid (t, \alpha_i) > 0 \text{ for } i = 1, \dots, \ell \text{ and } (t, \alpha_0) < 1\}.\end{aligned}$$

The hyperplanes $\{H_{\alpha_1,0},\ldots,H_{\alpha_\ell,0},H_{-\alpha_0,1}\}$ are called the *walls* of $\mathcal{A}_0$.

Observe that Theorem 11-3 asserts that W_{aff} is a Coxeter group with the generators being the reflections in the walls of $\mathcal{A}_0$. This is analogous to the Coxeter description of the Weyl group $W = W(\Delta)$ given in Remark 1 of §6-1. In that case, we used the reflections in the walls $\{H_{\alpha_1},\ldots,H_{\alpha_\ell}\}$ of the fundamental chamber C_0. We can duplicate, for alcoves, the study of Weyl chambers done in Chapter 4. Now W_{aff} permutes the hyperplanes $\{H_{\alpha,k}\}$ and, hence, the alcoves. As we observed at the end of §11-4, W_{aff} is generated by $\{s_0,s_1,\ldots,s_\ell\}$. As in §4-2, we can define length in W_{aff} with respect to $\{s_0,s_1,\ldots,s_\ell\}$ and show that length can be characterized by:

Proposition A *$\ell(\varphi) =$ the number of hyperplanes from $\{H_{\alpha,k}\}$ separating $\mathcal{A}_0$ and $\varphi\cdot\mathcal{A}_0$.*

As in §4-6, we can also show that:

Proposition B *W_{aff} acts freely and transitively on the alcoves.*

In closing, we note one further affine analogue of the results in Chapter 4. The following fact will be important in §12-4. Consider

$$\begin{aligned}\overline{\mathcal{A}_0} &= \{t\in\mathbb{E} \mid 0\le (t,\alpha)\le 1 \text{ for all } \alpha\in\Delta^+\}\\ &= \{t\in\mathbb{E} \mid (t,\alpha_i)\ge 0 \text{ for } i=1,\ldots,\ell \text{ and } (t,\alpha_0)\le 1\}\end{aligned}$$

the closure of $\mathcal{A}_0$. By an argument analogous to that in §4-6, we can establish that

$$(*)\qquad \mathbb{E} = \bigcup_{\varphi\in W_{\text{aff}}} \varphi\cdot\overline{\mathcal{A}_0},$$

i.e., every W_{aff} orbit in $\mathbb{E}$ contains an element of $\overline{\mathcal{A}_0}$.

By arguments analogous to those in §5-2, this assertion can be even further strengthened. For every subset $I\subset\{0,1,\ldots,\ell\}$, we can define the parabolic subgroup

$$W_{\text{aff},I}\subset W_{\text{aff}}$$

and show that every isotropy subgroup of W_{aff} is isomorphic to such a subgroup. In particular, if we decompose

$$\overline{\mathcal{A}_0} = \coprod_I \mathcal{A}_I,$$

where $\mathcal{A}_I$ is defined in a manner analogous to C_I in §5-2, then the isotropy group of each element of $\mathcal{A}_I$ is $W_{\text{aff},I}$. This leads to a decomposition

$$(**)\qquad \mathbb{E} = \coprod_I [\mathcal{A}_I \times (W_{\text{aff}}/W_{\text{aff},I})],$$

which is a strengthening of $(*)$.

11-6 The order of Weyl groups

Let $\Delta \subset \mathbb{E}$ be an irreducible essential crystallographic root system. Let $W = W(\Delta)$ and $W_{\mathrm{aff}} = W_{\mathrm{aff}}(\Delta)$ be its associated Weyl group and affine Weyl group, respectively. In this section, we demonstrate how to use W_{aff} to derive a formula for $|W|$ that involves only data from the root system Δ. For more details on the arguments of this section, consult Bott [1] and Iwahori-Matsumoto [1]. Recall from §11-2 that, given a fundamental system $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$, we have a uniquely determined highest root α_0 (with respect to Σ) with an expansion

$$\alpha_0 = h_1\alpha_1 + \cdots + h_\ell\alpha_\ell,$$

where the coefficients are the same for each choice of Σ. Let $\mathcal{Q} \subset \mathcal{P}$ be the root lattice and weight lattice, respectively, of Δ. The integer

$$c = |\mathcal{P}/\mathcal{Q}| = \det[(\alpha_i^\vee, \alpha_j)]_{\ell\times\ell}$$

was determined for irreducible crystallographic root systems in §9-5. The formula to be proved is:

Theorem **(Weyl)** $|W| = (\ell!)(\prod h_i)c.$

The proof of the theorem will involve the affine Weyl group and its action on $\mathbb{E}$. Recall that $W_{\mathrm{aff}} = \mathcal{Q}^\vee \rtimes W$, where W is the Weyl group and $\mathcal{Q}^\vee \subset \mathbb{E}$ is the coroot lattice interpreted as translations on $\mathbb{E}$. Every element of W_{aff} has a unique expression $\phi = T(d)\varphi$, where $\varphi \in W$ and $T(d)$ is the translation induced by $d \in \mathcal{Q}^\vee$. The action of W_{aff} on $\mathbb{E}$ is given for $\phi = T(d)\varphi \in W_{\mathrm{aff}}$ by

$$\phi \cdot x = \varphi \cdot x + d.$$

The affine Weyl group $W_{\mathrm{aff}} = W_{\mathrm{aff}}(\Delta) = \mathcal{Q}^\vee \rtimes W$ can be expanded to a slightly larger group $\widehat{W}_{\mathrm{aff}}$ by replacing the coroot lattice $\mathcal{Q}^\vee$ with the coweight lattice $\mathcal{P}^\vee$. This is the first mention of the *coweight lattice.* It is the dual (see §9-4) of the root lattice $\mathcal{Q}$ and can be written

$$\mathcal{P}^\vee = \mathbb{Z}\omega_1^\vee \oplus \cdots \oplus \mathbb{Z}\omega_\ell^\vee,$$

where $\{\omega_1^\vee, \ldots, \omega_\ell^\vee\}$ are the *fundamental coweights,* i.e., the duals of the fundamental roots $\{\alpha_1, \ldots, \alpha_\ell\}$

$$(\omega_i^\vee, \alpha_j) = \delta_{ij}.$$

The inclusion $\mathcal{Q} \subset \mathcal{P}$ dualizes to give an inclusion $\mathcal{Q}^\vee \subset \mathcal{P}^\vee$. We then define the *extended affine Weyl group*

$$\widehat{W}_{\mathrm{aff}} = \mathcal{P}^\vee \rtimes W.$$

There is a normal inclusion $W_{\mathrm{aff}} \lhd \widehat{W}_{\mathrm{aff}}$ and the action of W_{aff} on $\mathbb{E}$, as given above, extends to an action of $\widehat{W}_{\mathrm{aff}}$ on $\mathbb{E}$.

The alcoves of $\mathbb{E}$ were introduced in §11-5. The action of $\widehat{W}_{\mathrm{aff}}$ on $\mathbb{E}$ induces an action on the alcoves, and we shall use this action to prove the theorem. The action

of $W_{\text{aff}} \subset \widehat{W}_{\text{aff}}$ on the alcoves was already discussed in §11-5. It was observed that $W_{\text{aff}} \subset \widehat{W}_{\text{aff}}$ acts simply and transitively on the alcoves of $\mathbb{E}$.

We can define a complement (in $\widehat{W}_{\text{aff}}$) to W_{aff}. Let

$$\begin{aligned} \mathcal{A}_0 &= \{t \in E \mid 0 < (t, \alpha) < 1 \text{ for all } \alpha \in \Delta^+\} \\ &= \{t \in E \mid (t, \alpha_i) > 0 \text{ for } i = 1, \dots, \ell \text{ and } (t, \alpha_0) < 1\} \end{aligned}$$

be the fundamental alcove and let

$$\Omega = \{\varphi \in \widehat{W}_{\text{aff}} \mid \varphi \cdot \mathcal{A}_0 = \mathcal{A}_0\}.$$

We can then decompose $\widehat{W}_{\text{aff}}$ as a semidirect product $\widehat{W}_{\text{aff}} = W_{\text{aff}} \rtimes \Omega$.

The Weyl formula $|W| = (\ell!)(\prod h_i)c$ clearly follows from the next three lemmas. The first lemma is a straightforward consequence of the above discussion.

Lemma A $c = |\Omega|$.

Proof We have the sequence of identities

$$c = |\mathcal{P}/\mathcal{Q}| = |\mathcal{P}^\vee/\mathcal{Q}^\vee| = |\widehat{W}_{\text{aff}}/W_{\text{aff}}| = |\Omega|. \qquad \blacksquare$$

The proofs of the next two lemmas are more involved. Both lemmas involve the cube

$$\begin{aligned} \mathfrak{I} &= \left\{ \sum_i c_i \omega_i^\vee \;\middle|\; 0 \le c_i \le 1 \text{ for } i = 1, \dots, \ell \right\} \\ &= \{t \in \mathbb{E} \mid 0 \le (\alpha_i, t) \le 1 \text{ for } i = 1, \dots, \ell\}. \end{aligned}$$

Since $\mathfrak{I}$ is bounded by hyperplanes, it follows that each alcove is either inside $\mathfrak{I}$, or disjoint from it. We shall count the number of alcoves inside $\mathfrak{I}$ in two different ways. The following two lemmas, when combined with Lemma A, obviously produce the desired Weyl formula.

Lemma B *The number of alcoves in* $\mathfrak{I} = (\ell!)(\prod h_i)$.

Lemma C *The number of alcoves in* $\mathfrak{I} = |W|/|\Omega|$.

Proof of Lemma B We shall use a two-stage argument to verify that $(\ell!)(\prod h_i) =$ the number of alcoves in $\mathfrak{I}$. The two stages correspond to the factors $\prod h_i$ and $\ell!$, respectively.

(a) The Cube $\mathfrak{I}_0$ A smaller cube $\mathfrak{I}_0 \subset \mathfrak{I}$ is obtained by replacing the vertices $\{\omega_1^\vee, \dots, \omega_\ell^\vee\}$ by $\{(1/h_1)\omega_1^\vee, \dots, (1/h_\ell)\omega_\ell^\vee\}$. In other words,

$$\mathfrak{I}_0 = \left\{ \sum_i \left(\frac{c_i}{h_i}\right) \omega_i^\vee \;\middle|\; 0 \le c_i \le 1 \right\}.$$

$\mathfrak{I}$ consists of $\prod h_i$ copies of $\mathfrak{I}_0$. Moreover, each alcove in $\mathfrak{I}$ lies in one of these copies of $\mathfrak{I}_0$, and each copy contains the same number of alcoves. So Lemma B will be established if we can show:

(b) The number of alcoves in $\mathfrak{I}_0 = \ell!$ (i) We begin with a general decomposition result. Let $I =$ the unit interval $[0, 1]$. So $I^n = I \times \cdots \times I$ (n copies) is the n cube. We can decompose I^n into $n!$ identical copies of the n-simplex, where the different copies have disjoint interiors, i.e., the most that they have in common is their faces. We establish this fact by the following inductive argument.

We have a very useful decomposition for simplices. If the points $\{\epsilon_0, \epsilon_1, \ldots, \epsilon_q\}$ are in general position, then they determine a copy of a q simplex with these points as vertices. Namely, let

$$[\epsilon_0, \ldots, \epsilon_q] = \Big\{\sum_i x_i\epsilon_i \;\Big|\; \sum_i x_i = 1\Big\}.$$

If we call this copy Δ_q, then the product $\Delta_q \times I$ naturally decomposes into $q + 1$ copies of the $(q + 1)$-simplex. To locate these copies, let

$$\begin{aligned} A_0 &= (\epsilon_0, 0), \quad A_1 = (\epsilon_1, 0), \ldots, A_q = (\epsilon_q, 0) \\ B_0 &= (\epsilon_0, 1), \quad B_1 = (\epsilon_1, 1), \ldots, B_q = (\epsilon_q, 1). \end{aligned}$$

The various copies of the $(q + 1)$-simplex in $\Delta_q \times I$ are given by the simplices

$$[A_0, A_1, \ldots, A_{i-1}, A_i, B_i, B_{i+1}, \ldots, B_q] \quad (0 \le i \le q).$$

We note that the decomposition of $\Delta_q \times I$, and thus of I^n, is not unique. The ordering of the vertices $\{\epsilon_0, \epsilon_1, \ldots, \epsilon_q\}$ affects the decomposition produced.

Now, write $I^n = I^{n-1} \times I$ and suppose that I^{n-1} has been decomposed into $(n - 1)!$ copies of the $(n - 1)$-simplex. By taking each copy, Δ_{n-1}, of the $(n - 1)$-simplices in I^{n-1} and applying the above decomposition to $\Delta_{n-1} \times I$, we then produce a decomposition of I^n into $n!$ copies of the n-simplex. We can always arrange the orderings at each stage of the inductive argument (i.e., for the decompositions of $\Delta_q \times I$) so that one of the n-simplices appearing in the decomposition of I^n is $[e_0, e_1, \ldots, e_n]$, where

$$e_0 = (0, \ldots, 0)$$

$$e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \text{ with 1 lying in the } i\text{-th position } \{1 \le i \le n\}.$$

(ii) Next, we identify $\mathfrak{I}_0$ with I^ℓ and apply the decomposition result above to $\mathfrak{I}_0$. The canonical ℓ simplex just described can be identified with the closure $\overline{\mathcal{A}_0}$ of the fundamental alcove $\mathcal{A}_0$ because it will have vertices $\{0, (1/h_1)\omega_1^\vee, \ldots, (1/h_\ell)\omega_\ell^\vee\}$. So $\mathfrak{I}_0$ is a union of $\ell!$ copies of $\overline{\mathcal{A}_0}$, i.e., the union of $\ell!$ closures of alcoves.

Proof of Lemma C Since $W_{\text{aff}} \subset \widehat{W}_{\text{aff}}$ acts transitively on the alcoves, it follows that each alcove in $\Im$ is of the form $\phi \cdot \mathcal{A}_0$ for some $\phi \in \widehat{W}_{\text{aff}}$. The lemma follows from two facts.

(i) Given a fixed alcove $\mathcal{A}$, then $|\Omega| = \#\{\phi \in \widehat{W}_{\text{aff}}$ such that $\phi \cdot \mathcal{A}_0 = \mathcal{A}_0\}$;
(ii) $|W| = \#\{\phi \in \widehat{W}_{\text{aff}}$ such that $\phi \cdot \mathcal{A}_0 \in \Im\}$.

Proof of (i) We know that W_{aff} acts transitively on the alcoves. Consequently, there is an element of $\widehat{W}_{\text{aff}}$ mapping $\mathcal{A}_0$ onto each alcove. Moreover, any two elements of $\widehat{W}_{\text{aff}}$ mapping $\mathcal{A}_0$ onto a given alcove differ by an element of Ω because, if $\phi \cdot \mathcal{A}_0 = \psi \cdot \mathcal{A}_0$, then $\phi \cdot \psi^{-1} \in \Omega$.

Proof of (ii) Each $\phi \in \widehat{W}_{\text{aff}}$ can be written uniquely in the form $\phi = T(d)\varphi$, where $d \in \mathcal{P}^{\vee}$ and $\varphi \in W$. We shall show that each $\varphi \in W$ appears once and only once among the $\{\phi = T(d)\varphi\}$ that map $\mathcal{A}_0$ to $\Im$. This clearly suffices to establish (ii). We want to show that, given $\varphi \in W$, there exists one and only one $d \in P^{\vee}$ such that $T(d)\varphi$ maps $\mathcal{A}_0$ to $\Im$.

We shall work backwards. Pick $\phi = T(d)\varphi \in \widehat{W}_{\text{aff}}$ and suppose that $\phi \cdot t \in \Im$, where $t \in \mathcal{A}_0$. The relation $t \in \mathcal{A}_0$ can be reformulated as

$$(*) \qquad 0 < (\alpha_i, t) < 1 \text{ for } \alpha > 0 \quad \text{and} \quad -1 < (\alpha_i, t) < 0 \text{ for } \alpha < 0.$$

Also the relation $\phi \cdot t \in \Im$ is equivalent to asserting that

$$(**) \qquad 0 \leq (\alpha_i, \phi \cdot t) \leq 1 \quad \text{for } i = 1, \ldots, \ell.$$

The inequalities of $(*)$ and the identity $(\varphi \cdot t, \alpha_i) = (t, \varphi^{-1} \cdot \alpha_i)$ imply that

$$(*)' \qquad \begin{aligned} 0 < (\varphi \cdot t, \alpha_i) < 1 \quad & \text{if } \varphi^{-1} \cdot \alpha_i > 0 \\ -1 < (\varphi \cdot t, \alpha_i) < 0 \quad & \text{if } \varphi^{-1} \cdot \alpha_i < 0. \end{aligned}$$

Since $\phi \cdot t = \varphi \cdot t + d$, the inequalities of $(**)$ can be rewritten

$$(**)' \qquad 0 \leq (\alpha_i, \varphi \cdot t) + (\alpha_i, d) \leq 1 \quad \text{for } i = 1, \ldots, \ell.$$

Since $\mathcal{Q}$ and $\mathcal{P}^{\vee}$ are dual lattices, we have $(\alpha_i, d) \in \mathbb{Z}$. Moreover, the exact values of (α_i, d) are forced by $(*)'$ and $(**)'$. Namely, if $\varphi^{-1} \cdot \alpha_i > 0$, then $(\alpha_i, d) = 0$ while, if $\varphi^{-1} \cdot \alpha_i < 0$, then $(\alpha_i, d) = 1$. Thus d is uniquely determined by φ. ∎

12 Subroot systems

In this chapter we explain, and justify, an algorithm for determining the closed subroot systems of a given crystallographic root system. The arguments of this chapter provide a nice illustration of the effectiveness of passing from the ordinary Weyl group to the affine Weyl group when studying root systems.

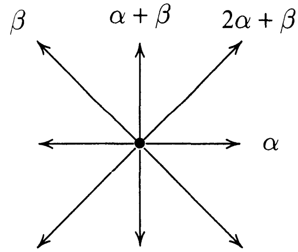
12-1 The Borel-de Siebenthal theorem

Given a root system, a natural question is to ask for all subroot systems. Borel and de Siebenthal [1] answered a more limited version of this question in the case of crystallographic root systems. Their results are concerned with closed subroot systems.

Definition: A subroot system $\Delta' \subset \Delta$ is *closed* if, for any $\alpha, \beta \in \Delta'$, $\alpha + \beta \in \Delta$ implies $\alpha + \beta \in \Delta'$. (In other words, $\alpha + \beta \in \Delta'$ whenever $\alpha + \beta$ is a root.)

The concern with closed subroot systems arises out of Lie theory. If we convert crystallographic root systems Δ into semisimple Lie algebras $L(\Delta)$ as in Appendix D, then asserting that $\Delta' \subset \Delta$ is closed is equivalent to asserting that $L(\Delta') \subset L(\Delta)$ is a sub-Lie algebra. So determining the closed subroot systems of a crystallographic root system amounts to determining the semisimple sub-Lie algebras of a semisimple Lie algebra.

The question of determining closed subroot systems is a matter of some delicacy. Consider, for example, the root system B_2.



The short roots $\{\mp\alpha, \mp(\alpha+\beta)\}$ form a subroot system $A_1 \times A_1 \subset B_2$. The long roots $\{\mp\beta, \mp(2\alpha+\beta)\}$ also form a subroot system $A_1 \times A_1 \subset B_2$. But the "short version" of $A_1 \times A_1$ is not closed, whereas the "long version" is closed. So the property of a subroot system being closed depends not only on its type (e.g. $A_1 \times A_1$), but also on the precise manner in which the subroot system sits inside the ambient root system. We note that, as in the above example, the long roots of a root system always form a closed subroot system.

The action of W on Δ permutes the closed subroot system of Δ. Two sets $S, S' \subset \mathbb{E}$ are said to be W-*equivalent* if there exists $\varphi \in W$ such that $\varphi \cdot S = S'$. We shall consider closed root systems of Δ classified up to W equivalence. The closed subroot systems of Δ form a partially ordered set. The Borel-de Siebenthal result is concerned with the maximal closed subroot systems of irreducible root systems. As we shall see, all the closed subroot systems of an arbitrary crystallographic root

system can be determined once we have a recipe for determining the maximal ones.

***Theorem* (Borel-de Siebenthal)** *Let Δ be an irreducible crystallographic root system. Let $\{\alpha_1, \ldots, \alpha_\ell\}$ be a fundamental system. Let α_0 be the highest root of Δ with respect to $\{\alpha_1, \ldots, \alpha_\ell\}$. Expand*

$$\alpha_0 = \sum_{i=1}^{\ell} h_i \alpha_i .$$

Then the maximal closed subroot systems of Δ (up to W equivalence) are those with fundamental systems

(i) $\{\alpha_1, \alpha_2, \ldots, \hat{a}_i, \ldots, \alpha_\ell\}$ *where* $h_i = 1$;
(ii) $\{-\alpha_0, \alpha_1, \ldots, \hat{a}_i, \ldots, \alpha_\ell\}$ *where* $h_i = p$ *(prime).*

(We use "$\wedge$" to denote elimination.) This theorem provides a simple algorithm for calculating the maximal closed subroot systems. For each irreducible crystallographic root system $\{A_\ell, \ldots, G_2\}$, take its Affine Dynkin Diagram as given in §11-4. The set of nodes of is $\{-\alpha_0, \alpha_1, \ldots, \alpha_\ell\}$. The table below gives the affine Dynkin Diagrams with an integer assigned to each vertex $\{\alpha_1, \ldots, \alpha_\ell\}$, namely, its coefficient in the expansion $\alpha_0 = \sum_{i=1}^{\ell} h_i \alpha_i$. The table is a modification of the information given in §11-2 and §11-4. A table of the coefficients in the expansion $\alpha_0 = \sum_{i=1}^{\ell} h_i \alpha_i$ for the various root systems was given in Table 4 of §11-2. The Affine Dynkin Diagram with nodes $\{-\alpha_0, \alpha_1, \ldots, \alpha_\ell\}$ was given in Table 6 of §11-4. Table 7 below combines this information.

We have indicated by "$\otimes$" the node corresponding to the extra root $-\alpha_0$. The Borel-de Siebenthal theorem tells us how to obtain, for each irreducible crystallographic root system, the Dynkin diagram of each maximal closed subroot systems.

(i) When $h_i = 1$ delete the nodes $-\alpha_0$ and α_i.
(ii) When $h_i = p$ (a prime) delete the node α_i.

By combining the information with the table in §10-5, it is easy to see that, in the case of irreducible crystallographic root systems of rank ℓ, we obtain the following list of maximal closed root systems.

Δ	Rank $\ell - 1$	Rank ℓ
A_ℓ	$A_i \times A_{\ell-i-1}$ $(0 \le i \le \ell - 1)$	
B_ℓ	$B_{\ell-1}$	$D_\ell, B_i \times D_{\ell-i}$ $(1 \le i \le \ell - 2)$
C_ℓ	$A_{\ell-1}$	$C_i \times C_{\ell-i}$ $(1 \le i \le \ell - 1)$
D_ℓ	$A_{\ell-1}, D_{\ell-1}$	$D_i \times D_{\ell-1}$ $(2 \le i \le \ell - 2)$
E_6	D_5	$A_1 \times A_5, A_2 \times A_2 \times A_2$
E_7	E_6	$A_1 \times D_6, A_7, A_2 \times A_5$
E_8		$D_8, A_1 \times E_7, A_8,$ $A_2 \times E_6, A_4 \times A_4$
F_4		$A_1 \times C_3, B_4, A_2 \times A_2$
G_2		$A_1 \times A_1, A_2$

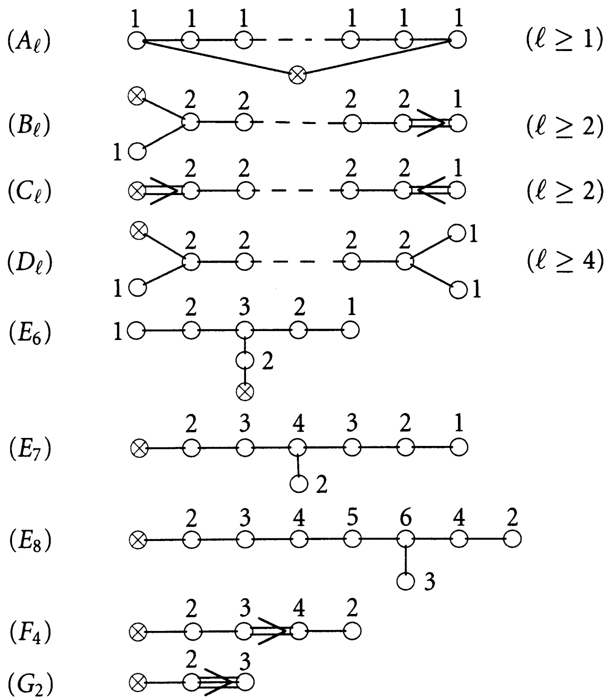


Table 7: Affine Dynkin diagrams

If a root system is decomposable, say $\Delta = \Delta_1 \coprod \Delta_2$, then it is easy to see that any closed subroot system of Δ is of the form $\Delta' = \Delta_1' \coprod \Delta_2'$, where $\Delta_1' \subset \Delta_1$ and $\Delta_2' \subset \Delta_2$ are closed subroot systems. So we can apply the above theorem to decomposable root systems. Namely, if $\Delta = \Delta_1 \coprod \cdots \coprod \Delta_n$ where $\Delta_1, \ldots, \Delta_n$ are irreducible root systems, then a maximal closed subroot system of Δ is of the form

$$\Delta' = \Delta_1' \coprod \cdots \coprod \Delta_n'$$

where, for some $1 \leq k \leq n$,

(i) $\Delta_i' = \Delta_i$ if $i \neq k$;
(ii) Δ_k' is a maximal root system of Δ_k, and is one of the cases given in the previous chart.

We can apply the Borel-de Siebenthal theorem recursively (using downward induction on $|\Delta|$) and obtain all possible closed subroot systems of a given Δ. We note, however, that such a list only answers the question of existence of closed subroot systems. We are still left with the problem of determining (up to W equivalence) the exact number of distinct closed subroot systems of a given type. For example, for each root $\alpha \in \Delta$, we have the closed root system $A_1 = \{\pm\alpha\}$. But any two short roots, and any two long roots, determine equivalent copies of A_1. So there are, at most, two nonequivalent copies of A_1.

12-2 The subroot system $\Delta(t)$

Given a crystallographic root system $\Delta \subset \mathbb{E}$ then, for each $t \in \mathbb{E}$, we can define the subset

$$\Delta(t) \subset \Delta$$
$$\Delta(t) = \{\alpha \in \Delta \mid (\alpha, t) \in \mathbb{Z}\}.$$

These subsets are the key to proving the Borel-de Siebenthal theorem. The rest of the chapter will be devoted to the study of the sets $\Delta(t)$. We shall show that they are closed subroot systems, and that they include every maximal closed subroot system. We then prove the Borel-de Siebenthal theorem by determining the possibilities for $\Delta(t)$. We close this section by proving the first of these assertions about $\Delta(t)$.

Proposition *For each $t \in \mathbb{E}$, $\Delta(t)$ is a closed subroot system.*

Proof First of all, $\Delta(t)$ is a root system satisfying the axioms (B-1) and (B-2) from §2-1. Obviously, $\alpha \in \Delta(t)$ implies $-\alpha \in \Delta(t)$. So (B-1) is satisfied. Regarding the invariance property (B-2), pick $\alpha, \beta \in \Delta(t)$. Then $s_\alpha \cdot \beta = \beta - \langle \alpha, \beta \rangle \alpha$, where $\langle \alpha, \beta \rangle \in \mathbb{Z}$. So $(s_\alpha \cdot \beta, t) \in \mathbb{Z}$. Secondly, the property of $\Delta(t)$ being closed is obvious. ■

12-3 Maximal subroot systems

In this section, we show that any maximal closed subroot system of a crystallographic root system $\Delta \subset \mathbb{E}$ is of the form $\Delta(t)$ for some $t \in \mathbb{E}$. This result is based on the fact that we can distinguish between closed root systems by using their associated root lattices. Given subroot systems $\Delta' \subset \Delta''$ of Δ, then we have an inclusion $\mathcal{Q}' \subset \mathcal{Q}''$ between their root lattices. It is quite possible to have $\mathcal{Q}' = \mathcal{Q}''$ even if $\Delta' \neq \Delta''$. Consider the example $A_1 \times A_1 \subset B_2$ discussed in §12-1. When we take the long root copy of $A_1 \times A_1$ (i.e., the closed copy), then its root lattice is distinct from that of B_2. However, when we take the short root copy (i.e., the nonclosed copy), then its root lattice is the same as that of B_2. This example exhibits a general fact characteristic of closed subroot systems.

Proposition *Let $\Delta' \subset \Delta''$ be subroot systems of Δ. Let $\mathcal{Q}' \subset \mathcal{Q}''$ be their associated root lattices. If Δ' is closed, then $\Delta' = \Delta''$ if and only if $\mathcal{Q}' = \mathcal{Q}''$.*

Proof Suppose $\mathcal{Q}' = \mathcal{Q}''$. To show $\Delta' = \Delta''$ we must show $\Delta'' \subset \Delta'$. Pick $\alpha \in \Delta''$. Since $\Delta'' \subset \mathcal{Q}'' = \mathcal{Q}'$, we can expand

$$(*) \qquad \alpha = \lambda_1\alpha_1 + \cdots + \lambda_m\alpha_m,$$

where $0 \neq \lambda_i \in \mathbb{Z}^+$ and $\{\alpha_1, \ldots, \alpha_m\}$ is a linearly independent set from Δ'. Replace α_i by $-\alpha_i$, if necessary, to ensure $\lambda_i \geq 0$. We now prove, by induction on

$\sum_{i=1}^{m} \lambda_i$, that any element from Δ'' possessing such an expansion belongs to Δ'. If $\sum_{i=1}^{m} \lambda_i = 1$ then $\alpha = \alpha_i$ for some $\alpha_i \in \Delta'$. Now, consider general $\alpha \in \Delta''$ having an expansion such as $(*)$. It suffices to prove

$$(**) \qquad \text{There exists } 1 \leq i \leq m \text{ such that } \alpha - \alpha_i \in \Delta'.$$

For then, by induction, $\alpha - \alpha_i \in \Delta'$ and so $\alpha = (\alpha - \alpha_i) + \alpha_i \in \Delta'$. To prove $(**)$ observe, first of all, that $(\alpha, \alpha_i) > 0$ for some i. Otherwise $(\alpha, \alpha) = \sum_{i=1}^{m} \lambda_i(\alpha, \alpha_i) \leq 0$ and so $\alpha = 0$, a contradiction. Secondly, apply Lemma 11-2. ■

We can use the proposition to show that any maximal closed subroot system is of the form $\Delta(t)$ for some $t \in \mathbb{E}$. For, suppose we have a proper closed subroot system.

$$\Delta' \subsetneqq \Delta.$$

We want to show that there exists $\Delta(t)$ so that

$$\Delta' \subset \Delta(t) \subsetneqq \Delta.$$

Since $\Delta' \subsetneqq \Delta$, we know, by the proposition, that their root lattices satisfy

$$\mathcal{Q}' \subsetneqq \mathcal{Q}.$$

If we take the dual lattices (see §11-4), we have

$$\mathcal{Q}^{\perp} \subsetneqq (\mathcal{Q}')^{\perp}.$$

Pick $t \in (\mathcal{Q}')^{\perp}$, where $t \notin \mathcal{Q}^{\perp}$. These properties tell us that $\Delta' \subset \Delta(t) \subsetneqq \Delta$.

12-4 Characterizations of the root systems $\Delta(t)$

We next describe the possibilities for the root systems $\Delta(t) \subset \Delta$. This is not quite a classification of such root systems because there are possible redundancies in the list we obtain. In §12-5 we shall further examine the list and eliminate redundancies in the case of the maximal root systems.

When we study the root systems $\Delta(t)$, we can reduce to the case $t \in \overline{\mathcal{A}_0}$, the closure of the fundamental alcove because we have already pointed out in §11-5 that every W_{aff} orbit in $\mathbb{E}$ contains an element from $\overline{\mathcal{A}_0}$. So to reduce to $t \in \overline{\mathcal{A}_0}$, it suffices to show that the equivalence class of $\Delta(t)$ only depends on the W_{aff} orbit of t.

Lemma *Given $x, y \in \mathbb{E}$, if $x = \varphi \cdot y$ for some $\varphi \in W_{\text{aff}}$, then $\Delta(x) = \phi \cdot \Delta(y)$ for some $\phi \in W_{\text{aff}}$.*

Proof We can write $W_{\text{aff}} = \mathcal{Q}^{\vee} \rtimes W$. So we can reduce to $\varphi \in W$ or $\varphi \in \mathcal{Q}^{\vee}$. We consider the two cases separately.

(i) $\varphi \in W$: The relation $(\alpha, x) = (\alpha, \varphi \cdot y) = (\varphi^{-1} \cdot \alpha, y)$ tells us that $\varphi^{-1} \cdot \Delta(x) = \Delta(y)$. So the root systems are equivalent.

(ii) $\varphi \in \mathcal{Q}^\vee$: Then φ is translation by $d \in \mathcal{Q}^\vee$ and $x = \varphi \cdot y = y + d$. Since $\Delta \subset \mathcal{Q} \subset \mathcal{P}$ and $\mathcal{Q}^\vee = \mathcal{P}^\perp$, we know that $(\alpha, d) \in \mathbb{Z}$ for all $\alpha \in \Delta$. Thus $\Delta(y + d) = \Delta(y)$. ■

The possibilities for $\Delta(t)$ when $t \in \overline{\mathcal{A}_0}$ are linked to the decomposition $\overline{\mathcal{A}_0} = \coprod \mathcal{A}_I$ mentioned in §11-5, where I runs through the proper subsets of $\{0, 1, \ldots, \ell\}$. Here $t \in \mathcal{A}_I$ means that t satisfies:

$$(*) \qquad \begin{cases} (\alpha_0, t) = 1 & \text{if } 0 \in I \\ (\alpha_0, t) < 1 & \text{if } 0 \notin I \\ (\alpha_i, t) = 0 & \text{if } 1 \leq i \leq \ell \text{ and } i \in I \\ (\alpha_i, t) > 0 & \text{if } 1 \leq i \leq \ell \text{ and } i \notin I. \end{cases}$$

Choose a fundamental system $\{\alpha_1, \ldots, \alpha_\ell\}$ for Δ. Let

$$\widetilde{\alpha}_0 = -\alpha_0, \quad \text{the negative of the highest root}$$

$$\widetilde{\alpha}_i = \alpha_i \quad \text{for } 1 \leq i \leq \ell.$$

Proposition *If $t \in \mathcal{A}_I$, then $\Delta(t)$ is the root system with fundamental system $\{\widetilde{\alpha}_i\}_{i \in I}$.*

Proof First of all, the roots $\{\widetilde{\alpha}_i\}_{i\in I}$ belong to $\Delta(t)$ because the first two statements of $(*)$ tell us that $\widetilde{\alpha}_i(t) \in \mathbb{Z}$ for $i \in I$. Secondly, the set $\{\widetilde{\alpha}_i\}_{i\in I}$ is linearly independent, since $\{\alpha_1, \ldots, \alpha_\ell\}$ is linearly independent and all the coefficients in the expansion $\alpha_0 = \sum_{i=1}^{\ell} h_i \alpha_i$ are nonzero. Thus no proper subset of $\{-\alpha_0, \alpha_1, \ldots, \alpha_\ell\}$ is linearly dependent. Thirdly, it remains to show that every $\alpha \in \Delta(t)$ can be expanded in terms of $\{\widetilde{\alpha}_i\}_{i\in I}$ with all nonnegative or all nonpositive coefficients. Pick $\alpha \in \Delta(t)$. Since $t \in \overline{\mathcal{A}_0}$, we must have $0 \leq (\alpha, t) \leq 1$. So the only possibilities are $(\alpha, t) = 0, 1$.

(i) $(\alpha, t) = 0$: Suppose $\alpha \in \Delta^+$. Write $\alpha = \sum_{i=1} \lambda_i \alpha_i$, where $\lambda_i \geq 0$. Then the equation

$$0 = (\alpha, t) = \sum_{i=1}^{\ell} \lambda_i (\alpha_i, t)$$

and the last two assertions of $(*)$ tell us that $\lambda_i = 0$ if $i \notin I$. Thus α can be expanded in terms of $\{\widetilde{\alpha}_i\}_{i\in I}$ with nonnegative coefficients. Indeed, $\widetilde{\alpha}_0$ is not even needed. The argument for $\alpha \in \Delta^-$ is similar.

(ii) $(\alpha, t) = 1$: Suppose $\alpha \in \Delta^+$. Write $\alpha = \alpha_0 + (\alpha - \alpha_0)$. Now $\alpha_0 \geq \alpha$ tells us that

$$\alpha - \alpha_o \in \Delta^-.$$

Since $(\alpha_i, t) \geq 0$ for $1 \leq i \leq \ell$, it also tells us that $(\alpha_0, t) \geq (\alpha, t) = 1$. But $t \in \overline{\mathcal{A}_0}$ forces $(\alpha_0, t) \leq 1$, so we have

$$(\alpha_0, t) = 1$$

or, equivalently,

$$(\alpha - \alpha_0, t) = 0.$$

By applying the argument in (i), we know that $\alpha - \alpha_0$ can be expanded in terms of $\{\widetilde{\alpha}_i\}_{i \in I}$ with nonpositive coefficients. We also know that $0 \in I$ (i.e., $(\alpha_0, t) = 1$). So $\alpha = \alpha_0 + (\alpha - \alpha_0) = -\widetilde{\alpha}_0 + (\alpha - \alpha_0)$ can be expanded in terms of $\{\widetilde{\alpha}_i\}_{i \in I}$ with nonpositive coefficients. The argument for $\alpha \in \Delta^-$ is similar. ∎

12-5 Maximal root systems

We now prove the Borel-de Siebenthal theorem. By §12-2, if we want to determine the maximal closed subroot systems of Δ, then it suffices to look at the root systems $\Delta(t)$. By §12-3, we can even assume that $t \in \overline{\mathcal{A}_0}$. These root systems were described in §12-4. They are generated by proper subsets of $\{-\alpha_0, \alpha_1, \dots, \alpha_\ell\}$. We now examine the various possibilities. In each case, we use Δ' to denote the root system generated by the chosen roots and "$\wedge$" to denote elimination.

(I) Case $\{\alpha_0, \alpha_1, \dots, \hat{a}_i, \dots, \alpha_\ell\}$

(a) $i = 0$: Obviously, $\Delta' = \Delta$.

(b) $i > 0$ and $h_i = 1$: Again $\Delta' = \Delta$. By Proposition 12-3, it suffices to show that the root lattices agree, i.e., $\mathcal{Q}' = \mathcal{Q}$. In $\mathcal{Q}/\mathcal{Q}'$ the equations

$$\alpha_0 = \alpha_1 = \cdots = \hat{a}_i = \cdots = \alpha_\ell = 0$$

can be rewritten

$$\alpha_1 = \alpha_2 = \cdots = \alpha_i = \cdots = \alpha_\ell = 0$$

(i.e., replace $\alpha_0 = 0$ by $\alpha_i = 0$). So $\mathcal{Q}/\mathcal{Q}' = 0$.

(c) $i > 0$ and $h_i = p$ prime: this time the root system is maximal because its root lattice $\mathcal{Q}' \subset \mathcal{Q}$ satisfies $\mathcal{Q}/\mathcal{Q}' = \mathbb{Z}/p\mathbb{Z}$. So it is not possible to find a lattice $\mathcal{Q}' \subsetneqq \mathcal{L} \subsetneqq \mathcal{Q}$.

(d) $i > 0$ and $h_i = ab$, where $a, b > 1$: the root system is not maximal. Pick $x \in \overline{\mathcal{A}_0}$ such that $\Delta' = \Delta(x)$. Let $y = ax$. We claim that

$$\Delta(x) \subsetneqq \Delta(y) \subsetneqq \Delta.$$

The inclusions $\Delta(x) \subset \Delta(y) \subset \Delta$ are obvious. The inequality $\Delta(y) \neq \Delta$ follows from the fact that

$$(*) \qquad \alpha_i \notin \Delta(y).$$

To prove this result, observe that $\{\alpha_0, \alpha_1, \dots, \hat{a}_i, \dots, \alpha_\ell\} \subset \Delta(x)$ where $x \in \overline{\mathcal{A}_0}$ forces the equations

$$(\alpha_0, x) = 1$$
$$(\alpha_j, x) = 0 \quad j \neq i.$$

From these we deduce that $(h_i\alpha_i, x) = 1$, and hence that

$$ab(\alpha_i, x) = 1.$$

So $(\alpha_i, y) = a(\alpha_i, x) = a(1/ab) = 1/b \notin \mathbb{Z}$, which concludes the proof of $(*)$.

By repeated applications of $(**)$ from the proof of Proposition 12-3, we can find $\alpha \in \Delta$ where the coefficient of α_i in the expansion $\alpha = \sum_{i=1}^{\ell} \lambda_j \alpha_j$ is b, i.e., $\lambda_i = b$.

$$(**) \qquad \alpha \in \Delta(y) \quad \text{and} \quad \alpha \notin \Delta(x).$$

For, by arguing as above, we obtain the equalities

$$(\alpha, x) = (b\alpha_i, x) = b(\alpha_i, x) = b(1/ab) = 1/a$$
$$(\alpha, y) = (b\alpha_i, ax) = ab(\alpha_i, x) = ab(1/ab) = 1.$$

(II) Case $\{\alpha_0, \alpha_1, \ldots, \hat{a}_i, \ldots, \hat{a}_j, \ldots, \alpha_\ell\}$

(a) $h_i = h_j = 1$: these root systems are maximal. First of all, $\Delta' \neq \Delta$ because $\operatorname{rank} \Delta' \leq \ell - 1 < \ell = \operatorname{rank} \Delta$. Moreover, by the first paragraph of this section, the only way to obtain a larger closed root system would be to add α_i or α_j to Δ'. However, by the argument in case (I), the resulting root system would be all of Δ.

On the other hand, the root systems obtained by deleting α_i and α_j are not all distinct. There are redundancies. We can reduce to the case

$$(* * *) \qquad i = 0.$$

For, suppose $\Delta' = \Delta(x)$, where $x \in \overline{\mathcal{A}_0}$. The decomposition $\overline{\mathcal{A}_0} = \coprod \mathcal{A}_I$ gives $\overline{\mathcal{A}_0}$, a simplex structure. Now x lies on the edge

$$\alpha_0 = 1, \quad \alpha_1 = \cdots = \hat{a}_i = \cdots = \hat{a}_j = \cdots = \alpha_\ell = 0,$$

with the vertices

$$\alpha_0 = 1, \quad \alpha_1 = \cdots = \hat{a}_i = \cdots = \alpha_\ell 0$$
$$\alpha_0 = 1, \quad \alpha_1 = \cdots = \hat{a}_j = \cdots = \alpha_\ell = 0$$

as endpoints. Denote these vertices by y and z. As observed above, $\Delta(y) = \Delta(z) = \Delta$. In particular, $\mp y \in \Omega^\perp$. So we can translate x by $-y$ without affecting $\Delta(x)$. After translating, x lies on an edge emanating from the origin. We can also apply an element of W to move the edge into $\overline{C_0}$, the closure of the fundamental chamber and, hence, into $\overline{\mathcal{A}_0}$. We now have reduced to $i = 0$, since the origin is one of the endpoints of the edge.

(b) $h_i > 1$ or $h_j > 1$: Assume $h_i > 1$. If we add α_j to Δ', we obtain a larger closed root system. Moreover, by the argument in case (I), this larger root system is not all of Δ. So Δ' cannot be maximal.

(III) Case where we delete more than 2 roots from $\{\alpha_0, \ldots, \alpha_\ell\}$ We can assume that at least three roots have been deleted. So if we add one root, we obtain a bigger closed root system. Such a root system is contained in the root system analyzed in case (II). In particular, such root systems are proper. So our extension of Δ' is also proper. Thus Δ' is not maximal.

13 Formal identities

Let $\Delta \subset \mathbb{E}$ be a crystallographic root system, and let Ω be the root lattice of Δ. Most of this chapter will be devoted to producing certain formal identities in the group ring of Ω. The main result of this chapter will be an identity in the polynomial ring $\mathbb{Z}[t]$ that provides a nontrivial relation between length in $W = W(\Delta)$ and height in Δ. Such an identity is of interest in its own right. However, the main motivation for such a formula is invariant theory. Its importance in invariant theory will be demonstrated in §27-2, when it is used to calculate the degrees of Weyl groups. The results of this chapter were first proved in MacDonald [2].

13-1 The MacDonald identity

Let $\Delta \subset \mathbb{E}$ be a crystallographic root system. Let $\Omega \subset \mathbb{E}$ be the root lattice of Δ (see §9-2). We define the group ring $\mathbb{Z}[\Omega]$ as follows.

Definition: $\mathbb{Z}[\Omega]$ is the free $\mathbb{Z}$ module with basis $\{e^x \mid x \in \Omega\}$ and multiplication determined by $e^x e^y = e^{x+y}$.

This is the usual group ring of Ω. We have, however, used "exponentiation" in order to write Ω as a multiplicative group. The action of $W = W(\Delta)$ on Ω induces an action on $\mathbb{Z}[\Omega]$ by the rule

$$\varphi \cdot e^x = e^{\varphi \cdot x}.$$

Lastly, we note that $\mathbb{Z}[\Omega]$ is an integral domain. To see this, observe, first of all, that we can totally order the elements of Ω. Choose a fundamental system $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$ of Δ. Thus $\Omega = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_\ell$, i.e., every $x \in \Omega$ can be expanded $x = c_1\alpha_1 + \cdots + c_\ell\alpha_\ell$. We totally order the elements of Ω by means of the first difference in the coefficients $c_1, \ldots, c_\ell$. The order on Ω imposes an order on the basis elements $\{e^x \mid x \in \Omega\}$. Given $\alpha \neq 0$, $\beta \neq 0$ in $\mathbb{Z}[\Omega]$, write

$$\alpha = ae^x + \text{lower terms} \quad (a \neq 0)$$

$$\beta = be^y + \text{lower terms} \quad (b \neq 0).$$

Then $\alpha\beta = abe^{x+y}+$ lower terms, in particular $\alpha\beta \neq 0$.

Most of the chapter is devoted to proving a formal identity in $\mathbb{F}[t]$, where $\mathbb{F} =$ the field of fractions of $\mathbb{Z}[\Omega]$. Given a fundamental system $\Sigma \subset \Delta$, we have the associated partition $\Delta = \Delta^+ \coprod \Delta^-$ of Δ into positive and negative roots. We can also define the length, $\ell(\varphi)$, of each element of $W = W(\Delta)$ with respect to Σ. The following (amazing) identity then holds in $\mathbb{F}[t]$.

Theorem **(MacDonald)** $\sum_{\varphi \in W} t^{\ell(\varphi)} = \sum_{\varphi \in W} [\prod_{\alpha > 0} \frac{1 - te^{-\varphi \cdot \alpha}}{1 - te^{-\varphi}}]$.

We note that this identity is independent of the choice of the fundamental system $\Sigma \subset \Delta$. This reduces to the fact that any two fundamental systems are related by an element of $W(\Delta)$. In particular, the polynomial $\sum_{\varphi \in W} t^{\ell(\varphi)}$ is independent

of the choice of Σ. The point is that the length of any particular element in W may vary according to the fundamental system chosen, but the total number of elements of a given length in W is independent of such a choice because any two fundamental systems $\Sigma, \Sigma' \subset \Delta$ are related by an element $\varphi \in W$, i.e., $\varphi \cdot \Sigma = \Sigma'$. And φ conjugates elements of a given length with respect to Σ into elements of the same length with respect to Σ'.

The fundamental system $\Sigma \subset \Delta$ can also be used to define height, $h(\alpha)$, for each $\alpha \in \Delta$. By "specializing" the MacDonald identity, we can obtain a polynomial identity in $\mathbb{Z}[t]$ that relates height in Δ to length in $W(\Delta)$.

Corollary $\sum_{\varphi \in W} t^{\ell(\varphi)} = \prod_{\alpha>0} \frac{t^{h(\alpha)+1}-1}{t^{h(\alpha)}-1}$.

Again, even though both length and height depend on the choice of the fundamental system of Δ, the identity is actually independent of such a choice. We note that the crystallographic condition is needed in the identity to ensure that $h(\alpha) \in \mathbb{Z}$ for all α.

We have an imbedding $\Omega \subset \mathbb{E}$, where $\mathbb{E}$ is the Euclidean space containing Δ. We can repeat the above discussion of $\mathbb{Z}[\Omega]$ only with Ω replaced by $\mathbb{E}$. We then obtain the larger group ring $\mathbb{Z}[\Omega] \subset \mathbb{Z}[\mathbb{E}]$. In proving the Macdonald identity, it will be convenient to replace $\mathbb{F}$ with the field of fractions of $\mathbb{Z}[\mathbb{E}]$. So until the end of §13-5, we shall work with $\mathbb{E}$ rather than Ω, and with $\mathbb{Z}[\mathbb{E}]$ rather than $\mathbb{Z}[\Omega]$.

13-2 The element ρ

This section is, in essence, a footnote to the discussion in Chapter 4 of the action of Euclidean reflection groups on their associated root systems and chamber systems. In this chapter, we are only considering crystallographic root systems $\Delta \subset \mathbb{E}$. However, the discussion in this section actually holds even without the crystallographic condition. Let $\Sigma \subset \Delta$ be a fundamental system, and let $\Delta = \Delta^+ \coprod \Delta^-$ be the associated decomposition of Δ into positive and negative roots. Let

$$\rho = \frac{1}{2} \sum_{\alpha>0} \alpha.$$

For any subset $K \subset \Delta^+$, let

$$\rho_K = \rho - \sum_{\alpha \in K} \alpha.$$

It is very useful to keep in mind that ρ_K can also be written

$$\rho_K = \frac{1}{2} \sum_{\alpha>0} \pm\alpha \quad \text{where } \alpha \text{ has coefficient} \begin{cases} +1 & \text{if } \alpha \in \Delta^+ - K \\ -1 & \text{if } \alpha \in K. \end{cases}$$

Observe that $\rho = \rho_\phi$. Let $W = W(\Delta)$.

Lemma A *W permutes the elements $\{\rho_K\}$.*

Proof We have already observed that we form a given ρ_K by choosing, for each $\alpha \in \Delta^+$, either α or $-\alpha$, and then taking one half of the sum. In other words, we choose, for each reflecting hyperplane, one of the two orthogonal root vectors, and then take one half of the sum. Since $W(\Delta)$ permutes the reflecting hyperplane, it also permutes sets of orthogonal root vectors chosen as above. Consequently, it permutes sums such as above. ■

Each ρ_K either lies on a reflecting hyperplane, or in a chamber. We now study those ρ_K which lie in chambers. The fundamental system $\Sigma = \{\alpha_1, \dots, \alpha_\ell\}$ determines the fundamental chamber

$$\mathcal{C}_o = \{x \in \mathbb{E} \mid (\alpha_i, x) > 0 \text{ for } i = 1, \dots, \ell\}.$$

Lemma B *$\mathcal{C}_o$ contains a unique ρ_K, namely ρ.*

Proof First of all, we have

$$(*) \qquad \rho \in \mathcal{C}_o.$$

It suffices to show that, for each α_i in Σ, we have $(\alpha_i, \rho) > 0$. We have the standard reflection formula

$$s_{\alpha_i} \cdot \rho = \rho - \frac{2(\alpha_i, \rho)}{(\alpha_i, \alpha_i)} \alpha_i.$$

But s_{α_i} permutes $\Delta^+ - \{\alpha_i\}$, while $s_{\alpha_i} \cdot \alpha_i = -\alpha_i$ (see Lemma 4-3A). Consequently,

$$s_{\alpha_i} \cdot \rho = \rho - \alpha_i.$$

Thus $2(\alpha_i, \rho)/(\alpha_i, \alpha_i) = 1$ and $(\alpha_i, \rho) > 0$.

Secondly, we have

$$(**) \qquad \rho_K \in \mathcal{C}_o \quad \text{only if } \rho_K = \rho.$$

For, write $\rho_K = \rho - x$, where $x = \sum_{a \in K} \alpha$. We have

$$0 < \left(\rho - x, \frac{2\alpha_i}{(\alpha_i, \alpha_i)} \right) = 1 - \frac{2(\alpha_i, x)}{(\alpha_i, \alpha_i)}.$$

The first inequality follows from the fact that $\rho - x \in \mathcal{C}_o$. The second equality was established above. Since x is a sum of roots, we also have

$$\frac{2(\alpha_i, x)}{(\alpha_i, \alpha_i)} \in \mathbb{Z}.$$

So $(\alpha_i, x) \leq 0$ for each i. Since x is a sum of positive roots, we can write $x = \sum \lambda_i \alpha_i$, where $\lambda_i \geq 0$. But then

$$(x, x) = \sum_i \lambda_i (\alpha_i, x) \leq 0.$$

Thus $(x, x) = 0$ and $x = 0$. ■

By the results of §4-6, we know that each chamber $\mathcal{C}$ is of the form $\varphi \cdot \mathcal{C}_o$ for a unique $\varphi \in W$. It thus follows from Lemma B that:

Lemma C *Each chamber $\mathcal{C} = \varphi \cdot \mathcal{C}_o$ contains a unique ρ_K, namely $\varphi \cdot \rho$.*

Let $\ell(\varphi)$ denote the length of $\varphi \in W$ with respect to Σ. As was shown in §4-3, $\ell(\varphi)$ can be characterized as the number of positive roots transformed by φ into negative roots. We record, for future use,

Lemma D *If $K = \{\beta_1, \ldots, \beta_k\}$ are the positive roots transformed by φ into negative roots, then $\varphi \cdot \rho = \rho_K$.*

Lemma E *If $\rho_K = \varphi \cdot \rho$, then* $\det(\varphi) = (-1)^{\ell(\varphi)} = (-1)^{|K|}$.

Proof Regarding the first identity, if $\ell(\varphi) = k$, then $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$, where $\{s_{\alpha_1}, \ldots, s_{\alpha_k}\}$ are reflections. Since $\det(s_{\alpha_i}) = -1$, we have $\det(\varphi) = (-1)^k$. The second identity follows from Lemma D. ∎

13-3 The element Ψ

In §13-2, we defined the element ρ and, more generally, the element ρ_K for each subset $K \subset \Delta^+$. In this section we consider the elements

$$\Psi = \sum_{\varphi \in W} \det(\varphi) e^{\varphi \cdot \rho}$$

$$\Psi_K = \sum_{\varphi \in W} \det(\varphi) e^{\varphi \cdot \rho_K}$$

in $\mathbb{Z}[\mathbb{E}]$. First of all, many of the Ψ_K are trivial.

Lemma A *$\Psi_K = 0$ if ρ_K does not lie in a chamber.*

Proof If ρ_K does not lie in a chamber, then it must lie in a reflection hyperplane H_α. So $s_\alpha \cdot \rho_K = \rho_K$, where s_α is the reflection associated to H_α. Thus

$$\begin{aligned}
\Psi_K &= \sum_{\varphi \in W} \det(\varphi) e^{\varphi \cdot \rho_K} = \sum_{\varphi \in W} \det(\varphi) e^{\varphi s_\alpha \cdot \rho_K} \\
&= \det(s_\alpha) \sum_{\varphi \in W} \det(\varphi s_\alpha) e^{\varphi s_\alpha \cdot \rho_K} \\
&= \det(s_\alpha) \sum_{\varphi \in W} \det(\varphi) e^{\varphi \cdot \rho_K} \quad \text{(reindexing)} \\
&= -\Psi_K.
\end{aligned}$$

∎

We are left to consider Ψ_K where ρ_K belongs to a chamber. By §13-2, each chamber contains a unique ρ_K and $\rho_K = \varphi \cdot \rho$ for a unique $\varphi \in W$. The following lemma, therefore, describes the nonzero Ψ_K.

Lemma B *If $\rho_K = \varphi \cdot \rho$, then $\Psi_K = \det(\varphi)\Psi$.*

Proof

$$\begin{aligned}\Psi_K &= \sum_{\varphi\in W} \det(\phi)e^{\phi\cdot\rho_K} \\ &= \sum_{\varphi\in W} \det(\phi\varphi^{-1})e^{\phi\cdot\varphi^{-1}\cdot\rho_K} \quad \text{(reindexing)} \\ &= \det(\varphi^{-1})\sum_{\varphi\in W} \det(\phi)e^{\phi\cdot\rho} \quad (\rho_K = \varphi\cdot\rho) \\ &= \det(\varphi)\Psi.\end{aligned}$$

■

13-4 The Weyl identity

Let ρ and Ψ be defined as before. In this section, we produce an identity in $\mathbb{Z}[\mathbb{E}]$ asserting that Ψ can be expanded as a product. As in the previous sections, we continue to assume that $\Sigma \subset \Delta$ is a fundamental system and $\Delta = \Delta^+ \coprod \Delta^-$ is the associated decomposition of Δ into positive and negative roots.

***Theorem* (Weyl)** $\Psi = e^\rho \prod_{\alpha>0}(1 - e^{-\alpha})$.

We are only proving the Weyl identity as a step in the proof of the MacDonald identity, to be established in the next section. However, the Weyl identity is of interest in its own right. It arises in the representation theory of Lie algebras, and is usually called the Weyl Denominator formula.

We now set about proving the Weyl identity. To simplify notation, we let

$$\Psi_o = e^\rho \prod_{\alpha>0}(1 - e^{-\alpha}).$$

So we want to show $\Psi = \Psi_o$. First of all, we want to show that both Ψ and Ψ_o are skew. An element $x \in \mathbb{Z}[\mathbb{E}]$ is *skew* if $\varphi \cdot x = \det(\varphi)x$ for all $\varphi \in W$.

Lemma *Ψ is skew.*

Proof Given $\varphi \in W$, we have the identities

$$\begin{aligned}\varphi\cdot\Psi = \varphi\cdot\Big(\sum_{\varphi\in W}\det(\phi)e^{\phi\cdot\rho}\Big) &= \sum_{\varphi\in W}\det(\phi)e^{\varphi\cdot\phi\cdot\rho} \\ &= \det(\varphi^{-1})\sum_{\varphi\in W}\det(\varphi\cdot\phi)e^{\varphi\cdot\phi\cdot\rho} \\ &= \det(\varphi)\sum_{\varphi\in W}\det(\phi)e^{\phi\cdot\rho} \quad \text{(reindexing)} \\ &= \det(\varphi)\Psi.\end{aligned}$$

■

Lemma B *Ψ_o is skew.*

Proof Since W is generated by reflections, we can reduce to $\varphi = s_\beta$, a reflection. We want to show that $s_\beta \cdot \Psi_o = -\Psi_o$. Since $s_\beta = s_{-\beta}$, we can assume $\beta \in \Delta^+$. Recall that s_β permutes $\Delta^+ - \{\beta\}$, while $s_\beta \cdot \beta = -\beta$. Thus

$$(*) \qquad \prod_{\alpha>0}(1 - e^{-s_\beta \cdot \alpha}) = \frac{1 - e^\beta}{1 - e^{-\beta}} \prod_{\alpha>0}(1 - e^{-\alpha}).$$

We now have

$$\begin{aligned} s_\beta \cdot \Psi_o &= e^{s_\beta \cdot \rho} \prod_{\alpha>0}(1 - e^{-s_\beta \cdot \alpha}) \\ &= e^{\rho-\beta} \frac{1 - e^\beta}{1 - e^{-\beta}} \prod_{\alpha>0}(1 - e^{-\alpha}) \quad \text{by } (*) \\ &= -\frac{e^\rho}{e^\beta} \frac{e^\beta - 1}{1 - e^{-\beta}} \prod_{\alpha>0}(1 - e^{-\alpha}) \\ &= -e^\rho \prod_{\alpha>0}(1 - e^{-\alpha}) = -\Psi_o. \end{aligned}$$

■

If x is skew, then $\det(\phi)\phi(x) = x$ (since $\det(\phi) = \pm 1$). Thus

$$x = \frac{1}{|W|} \sum_{\varphi \in W} \det(\varphi)\varphi \cdot x.$$

In particular, by the above lemmas, we have

(i) $\Psi = \frac{1}{|W|} \sum_{\varphi \in W} \det(\varphi)\varphi \cdot \Psi$;
(ii) $\Psi_o = \frac{1}{|W|} \sum_{\varphi \in W} \det(\varphi)\varphi \cdot \Psi_o$.

We shall prove that $\Psi = \Psi_o$ by showing that the RHS of the above equalities agree. The reason for passing to these more complicated expressions is to enable us to take advantage of the results from §13-3.

Let ρ_K be defined as in §13-2. We can expand

(iii)

$$\begin{aligned} \Psi_o &= e^\rho \prod_{\alpha>0}(1 - e^{-\alpha}) \\ &= e^\rho \sum_{K \subset \Delta^+} (-1)^{|K|} e^{-[\sum_{\alpha \in K} \alpha]} \\ &= \sum_{K \subset \Delta^+} (-1)^{|K|} e^{\rho_K}. \end{aligned}$$

We now apply (i), (ii) and (iii), and the results of §13-2 and §13-3. We have

$$\begin{aligned}\Psi_o &= \sum_{K\subset\Delta^+} (-1)^{|K|}\Psi_K \quad \text{(by (ii) and (iii))}\\ &= \frac{1}{|W|}\sum_{\varphi\in W} \det(\varphi)\varphi(\Psi) \quad \text{(by Lemmas 13-2C, 13-3A, 13-3B)}\\ &= \Psi \quad \text{(by(i))}.\end{aligned}$$

13-5 The proof of the MacDonald identity

In this section, we prove Theorem 13-1. We shall continue to work in the field of fractions of $\mathbb{Z}[\mathbb{E}]$. The proof is analogous to, but more complicated than, the proof of the Weyl identity in §13-4. We expand the RHS of the MacDonald identity and, by making some key substitutions, convert it into the LHS. As in §13-4, we shall use the fact that $\Psi = \Psi_o$ is skew. Notably, the fact that Ψ_o is skew gives the identity

$$\prod_{\alpha>0}(1-e^{-\varphi\cdot\alpha}) = \frac{\Psi_0}{\det(\varphi)e^{\varphi\cdot\rho}}.$$

(We use the identity $\varphi\cdot\Psi_0 = \det(\varphi)\Psi_0$ and the Weyl identity from §13-4.) Substituting this equation into the RHS of the MacDonald identity, we obtain

$$\begin{aligned}\sum_{\varphi\in W}\left[\frac{1-te^{-\varphi\cdot\alpha}}{1-e^{-\varphi\cdot\alpha}}\right] &= \sum_{\varphi\in W}\frac{\det(\varphi)e^{\varphi\cdot\rho}}{\Psi_0}\prod_{\alpha>0}(1-te^{-\varphi\cdot\alpha})\\ &= \frac{1}{\Psi_0}\sum_{\varphi\in W}\det(\varphi)e^{\varphi\cdot\rho}\sum_{K\subset\Delta^+}(-t)^{|K|}e^{-\varphi[\sum_{\alpha\in K}\alpha]}\\ &= \frac{1}{\Psi_0}\sum_{K\subset\Delta^+}(-t)^{|K|}\Psi_K \quad \text{(by Lemma 13-2B)}\\ &= \frac{1}{\Psi_0}\sum_{\varphi\in W}\det(\varphi)t^{\ell(\varphi)}\varphi\cdot\Psi \quad \text{(by §13-3 and Lemma 13-2B)}\\ &= \frac{1}{\Psi_0}\sum_{\varphi\in W}\det(\varphi)^2t^{\ell(\varphi)}\Psi \quad (\Psi\text{ is skew})\\ &= \sum_{\varphi\in W}t^{\ell(\varphi)} \quad (\Psi=\Psi_o\text{ and }\det(\varphi)=\pm1).\end{aligned}$$

13-6 The proof of polynomial identity

In this section, we "specialize" the MacDonald identity and obtain the polynomial identity of Corollary 13-1. We shall prove the polynomial identity by substituting into the MacDonald identity. Let $\Omega\subset\mathbb{E}$ be the root lattice of Δ. In proving the

MacDonald identity, we worked over the fraction field of $\mathbb{Z}[\mathbb{E}]$. But an examination of the terms in the identity shows that the identity actually holds in $\mathbb{F}[t]$, where $\mathbb{F}$ is the fraction field of $\mathbb{Z}[\Omega] \subset \mathbb{Z}[\mathbb{E}]$. Moreover, if we eliminate denominators by multiplying both sides of the identity by $\prod_{\substack{\alpha>0 \\ \varphi\in W}} (1 - e^{-\varphi\cdot\alpha})$, then we can consider the identity as holding in $\mathbb{Z}[\Omega]$. We have an algebra homomorphism

$$\Phi\colon \mathbb{Z}[\Omega][t] \to \mathbb{Z}[t, t^{-1}]$$

determined by

$$\Phi(e^\alpha) = t^{-h(\alpha)}$$

for each $\alpha \in \Delta$. If we apply this homomorphism to the MacDonald identity, we obtain

$$(*) \qquad \sum_{\varphi\in W} t^{\ell(\varphi)} - \sum_{\varphi\in W} \left[\prod_{\alpha>0} \frac{1 - t^{h(\varphi\cdot\alpha)+1}}{1 - t^{h(\varphi\cdot\alpha)}} \right].$$

Most of the summands in the RHS of this equation disappear. We claim that

$$(**) \qquad \prod_{\alpha>0} \frac{1 - t^{h(\varphi\cdot\alpha)+1}}{1 - t^{h(\varphi\cdot\alpha)}} = 0 \quad \text{if } \varphi \neq 1.$$

Fix $\varphi \neq 1$. To prove $(**)$, it suffices to find $\alpha \in \Delta^+$ such that $h(\varphi \cdot \alpha) = -1$. Since $\varphi \neq 1$, we know that $\ell(\varphi) > 0$. By §4-3 we know that

$\ell(\varphi) =$ the number of positive roots converted by φ into negative roots.

Suppose that $\ell(\varphi) = k$, and that $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$ is a reduced expression in terms of the fundamental reflections $\{s_\alpha \mid \alpha \in \Sigma\}$. Theorem 4-3B tells us that the positive roots converted by φ into negative roots are

$$\{\alpha_k, s_{\alpha_k} \cdot \alpha_{k-1}, \ldots, (s_{\alpha_k} \cdots s_{\alpha_2}) \cdot \alpha_1\}.$$

Consider $\beta = (s_{\alpha_k} \cdots s_{\alpha_2}) \cdot \alpha_1$. Then $\varphi \cdot \beta = -\alpha_1$. So $h(\varphi \cdot \beta) = -1$.

Finally, observe that the polynomial identity follows from $(*)$ and $(**)$.

IV Pseudo-reflection groups

The next thirteen chapters deal with invariant theory and its extensions. The first two of these chapters, 14 and 15, begin that discussion by introducing and discussing pseudo-reflection groups. As we shall see, pseudo-reflection groups arise naturally during the discussion of invariant theory. Pseudo-reflection groups are generalizations of Euclidean reflection groups and provide a more natural context than Euclidean reflection groups in which to do invariant theory. This will first be clearly demonstrated in Chapter 18. Much of the remainder of the book is devoted to the relation between invariant theory and pseudo-reflection groups.

In Chapter 14, pseudo-reflections are introduced. In Chapter 15, the classifications obtained for pseudo-reflection groups are discussed. In particular, the Shephard-Todd classification of complex pseudo-reflection groups is outlined.

14 Pseudo-reflections

Reflections and reflection groups in Euclidean space have important generalizations. In this chapter, we discuss pseudo-reflections. This chapter, as well as the next, is preliminary to the study of invariant theory, since it is invariant theory that motivates the introduction of pseudo-reflections. Most of our discussion of invariant theory naturally takes place in the context of pseudo-reflection groups. However, it will take several chapters before we are able to demonstrate this point.

14-1 (Generalized) reflections

The generalization of Euclidean reflections to pseudo-reflections will take place in two stages. In this section, we extend the term "reflection" from Euclidean space to arbitrary vector spaces. Historically, this was the first generalization considered of an Euclidean reflection. In §14-2, we consider the more general notion of a "pseudo-reflection". It is pseudo-reflections that will be used in future chapters.

Let $\mathbb{F}$ be an arbitrary field, and let V be a finite dimensional vector space over $\mathbb{F}$. The following definitions are obviously patterned on the Euclidean reflection case.

Definition: A *reflection on* V is a diagonalizable linear isomorphism $s\colon V \to V$, which is not the identity map, but leaves a hyperplane $H \subset V$ pointwise invariant.

Definition: $G \subset \mathrm{GL}(V)$ is a *reflection group* if G is generated by its reflections.

As we shall see below, these definitions reduce, in the case $\mathbb{F} = \mathbb{R}$, to those previously considered for Euclidean space. We call H the *reflecting hyperplane* or *invariant hyperplane* of the reflection s.

All the eigenvalues of a reflection, with one exception, are equal to 1. We are interested in reflections of finite order. If $s\colon V \to V$ has order n, then its exceptional eigenvalue must be an n-th primitive root of unity ξ_n and $\det(s) = \xi_n$. Since different fields contain different roots of unity, the allowable values of n will vary with the field. For example:

$\mathbb{F} = \mathbb{R}$	$n = 2$
$\mathbb{F} = \mathbb{C}$	n arbitrary
$\mathbb{F} = \hat{\mathbb{Q}}_p$, the p-adic numbers	$\begin{cases} n \mid (p-1) & \text{for } p \text{ odd} \\ n = 2 & \text{for } p = 2 \end{cases}$

.

Given a reflection $s\colon V \to V$, if α is an eigenvector such that $s \cdot \alpha = \xi_n \alpha$, and $H \subset V$ is the hyperplane left pointwise invariant by s, then s has a decomposition

$$s \cdot x = x + \Delta(x)\alpha,$$

where $\Delta\colon V \to \mathbb{F}$ is a linear functional satisfying

$$H = \operatorname{Ker} \Delta$$

$$\Delta(\alpha) = \xi - 1.$$

Notation: We have simplified notation. The functional Δ really depends on two choices: s and α. So it should more properly be written $\Delta_{s,\alpha}$. The choice of s is, of course, crucial to the choice of Δ (and α). Given s, then α and Δ in the above decomposition are determined up to scalar multiple. This indeterminacy arises from the fact that we can always replace α by $k\alpha$ and Δ by $\frac{1}{k}\Delta$. Nevertheless, for the sake of notational simplicity, we have chosen to ignore these issues and denote the functional simply by Δ. The only point at which more explicit notation will be used is in the treatment of the Jacobian element Ω (see Chapter 20 for the definition). There we shall denote α and Δ by α_s and Δ_s, respectively.

If $s\colon V \to V$ is a reflection of order n, then $s^k\colon V \to V$ is also a reflection for $1 \leq k \leq n-1$. Observe that s^k has the same invariant hyperplane H as s while $s^k \cdot \alpha = \xi^k\alpha$. So if $s \cdot x = x + \Delta(x)\alpha$ as above, then we can decompose s^k by

$$s^k \cdot x = x + (1 + \xi + \cdots + \xi^{k-1})\Delta(x)\alpha.$$

There are several cases where reflections have canonical forms.

Example 1: $\mathbb{F} = \mathbb{R}$. A reflection $s\colon V \to V$ over $\mathbb{R}$, as defined above, is just a reflection in Euclidean space, as considered in previous chapters. Namely, given such a reflection, we can find an inner product on V and $\alpha \in V$ such that s satisfies the standard Euclidean reflection identity

$$(*) \qquad s \cdot x = x - \frac{2(\alpha, x)}{(\alpha, \alpha)}\alpha$$

for all $x \in V$. First of all, we can choose an inner product on V satisfying the identity

$$(s \cdot x, s \cdot y) = (x, y)$$

for all $x, y \in V$. This follows from the more general observation that, given a finite group $G \subset \mathrm{GL}(V)$, we can choose an inner product that is G-invariant, i.e.,

$$(\varphi \cdot x, \varphi \cdot y) = (x, y)$$

for all $x, y \in V$ and $\varphi \in G$. Just take any inner product $(x, y)'$ and replace it by

$$(x, y) = \sum_{\varphi \in G} (\varphi \cdot x, \varphi \cdot y)'.$$

To deal with the case of a single reflection s, let $G = \mathbb{Z}/2\mathbb{Z}$, the group generated by s.

Secondly, since s is of order 2, its only possible eigenvalues are ± 1. So we can pick an eigenvector $\alpha \in V$ such that $s \cdot \alpha = -\alpha$ and $V = H \oplus \mathbb{R}\alpha$. Moreover, α and H are orthogonal. For, given $x \in H$, we have

$$(\alpha, x) = (s \cdot \alpha, s \cdot x) = (-\alpha, x) = -(\alpha, x).$$

So $(\alpha, x) = 0$.

Lastly, with the above choices, s satisfies identity $(*)$. Just check the effect of the RHS of $(*)$ on α and on H.

Remark: Given a finite reflection group $G \subset \mathrm{GL}(V)$, where V is a finite dimensional vector space over $\mathbb{R}$, the above argument enables us to introduce an inner product on V such that all the reflections of G are Euclidean reflections satisfying $(*)$. Hence G can be regarded as a Euclidean reflection group.

Example 2: $\mathbb{F} = \mathbb{C}$. An argument similar to the one above, only using a positive definite Hermitian form rather than an inner product, yields that, in the case of a finite group G acting on a complex finite dimensional vector space V, we can choose a positive definite Hermitian form that is G-invariant. It then follows, again by an argument as above, that every reflection $s\colon V \to V$ of order n over $\mathbb{C}$ satisfies the identity

$$(**) \qquad s \cdot x = x + (\xi - 1)\frac{(\alpha, x)}{(\alpha, \alpha)}\alpha$$

for all $x \in V$, where ξ is a primitive n-th root of unity, α is an eigenvector such that $s \cdot \alpha = \xi \cdot \alpha$ and (x, y) is a positive definite Hermitian form satisfying $(s \cdot x, s \cdot y) = (x, y)$.

A number of concepts from the Euclidean reflection group case extend to the more general case under consideration. Two reflection groups $G \subset \mathrm{GL}(V)$ and $G' \subset \mathrm{GL}(V')$ will be said to be *isomorphic* if there exists a linear isomorphism $f\colon V \to V'$ conjugating G to G'. In other words,

$$fGf^{-1} = G'.$$

We have a concept of a reflection group $G \subset \mathrm{GL}(V)$ being reducible or irreducible. A reflection group $G \subset \mathrm{GL}(V)$ is *reducible* if it can be decomposed as $G = G_1 \times G_2$, where $G_1 \subset \mathrm{GL}(V)$ and $G_2 \subset \mathrm{GL}(V)$ are nontrivial subgroups generated by reflections from G. Otherwise, a reflection group will be said to be *irreducible*. A reflection group $G \subset \mathrm{GL}(V)$ is *essential* if only the origin of V is left fixed by all the elements of G. We can regard $G \subset \mathrm{GL}(V)$ as a representation of G. From the discussion in Appendix B and in §2-4, it follows that $G \subset \mathrm{GL}(V)$ is irreducible as a representation if and only if G is irreducible and essential as a reflection group.

A classification of finite reflection groups over any field $\mathbb{F}$ consists of a determination (up to isomorphism) of the finite essential irreducible reflection groups. We have already explained how all finite real reflection groups $G \subset \mathrm{GL}(V)$ can be converted into a finite Euclidean reflection group $G \subset O(\mathbb{E})$. As an extension of these ideas, it is also true that the classification for finite real reflection groups is the same as that for finite Euclidean reflection groups because it is clear that the above concepts of irreducible and essential agree when we identify real reflection groups with Euclidean reflection groups. Moreover, an "averaging" argument (analogous to that given in Example 1) converts an isomorphism $f\colon V \to V'$ between two reflection groups $G \subset \mathrm{GL}(V)$ and $G' \subset \mathrm{GL}(V')$ into an isomorphism

$\widetilde{f}\colon \mathbb{E} \longrightarrow \mathbb{E}'$ between the associated Euclidean reflection groups $G \subset O(\mathbb{E})$ and $G' \subset O(\mathbb{E}')$. We let $\widetilde{f} = \sum_{\varphi \in G} \varphi f \varphi^{-1}$.

In Chapter 15, we consider other classification results for (pseudo-) reflection groups.

14-2 Pseudo-reflections

The concept of a reflection generalizes to that of a pseudo-reflection. As we shall see in §14-3, this is only a true generalization for the "modular case". Let V be a finite dimensional vector space over a field $\mathbb{F}$.

Definition: A *pseudo-reflection* is a linear isomorphism $s\colon V \longrightarrow V$ that is not the identity map, but leaves a hyperplane $H \subset V$ pointwise invariant.

Definition: $G \subset \mathrm{GL}(V)$ is a *pseudo-reflection group* if G is generated by its pseudo-reflections.

Unlike a reflection, a pseudo-reflection is not required to be diagonalizable. Alternatively, a reflection is just a diagonalizable pseudo-reflection. There are many examples of nondiagonalizable pseudo-reflections. Notably, any *elementary matrix* (i.e., a matrix agreeing with the identity matrix except for a single nonzero entry off the diagonal) represents a nondiagonalizable pseudo-reflection. Consider, for example, $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$. Similarly, there are many examples of pseudo-reflection groups that are not reflection groups. It is well known that $\mathrm{SL}(V)$ is generated by elementary matrices. So $\mathrm{SL}(V)$ is a pseudo-reflection group, but not a reflection group. It is easy to deduce that the same must be true for $\mathrm{GL}(V)$.

When we restrict ourselves to pseudo-reflections of finite order, then most of the time they are diagonalizable. As will be explained in the next section, nondiagonalizable pseudo-reflections can only occur when $\operatorname{char} \mathbb{F} = p > 0$. Observe, for example, that the elementary matrices discussed above are of finite order only when $\operatorname{char} \mathbb{F} = p$. Moreover, even in this case, nondiagonalizable pseudo-reflections can only occur in special circumstances. In particular, they must be of order p. Again, this will be justified in the next section.

It will be useful to formulate the distinction between diagonalizable and nondiagonalizable in a slightly different way. As in the case of reflections, a pseudo-reflection has a decomposition

$$s \cdot x = x + \Delta(x)\alpha,$$

where $\Delta\colon V \longrightarrow \mathbb{F}$ is a linear functional. In this case, α generates $\mathrm{Im}(1 - s)$, i.e.,

$$\mathrm{Im}(1 - s) = \mathbb{F}\alpha,$$

while

$$H = \operatorname{Ker} \Delta,$$

where $H \subset V$ is the hyperplane on which the pseudo-reflection acts as the identity. Observe that s is diagonalizable (i.e., s is a reflection as defined in §14-1) if and

only if $\alpha \notin H$ (i.e., $\Delta(\alpha) \neq 0$). So α belonging (or not) to H distinguishes nondiagonalizable pseudo-reflections and reflections. In a slight abuse of notation, we shall refer to H as being the *reflecting hyperplane* or the *invariant hyperplane* of the pseudo-reflection s.

The definition of *essential* pseudo-reflection groups, *reducible* and *irreducible* pseudo-reflection groups, as well as of *isomorphisms* between pseudo-reflection groups, is analogous to that given in §14-1 for reflection groups.

14-3 The modular and nonmodular cases

Let V be a finite dimensional vector space over a field $\mathbb{F}$. When we deal with finite subgroups $G \subset \mathrm{GL}(V)$, we are really dealing with special cases of the representation theory of finite groups, in other words, with homomorphisms $\rho\colon G \to \mathrm{GL}(V)$. A brief survey of representation theory is given in Appendix B.

In this last section of Chapter 14, we want to focus on a concept from representation theory that plays an important role in invariant theory. Representation theory distinguishes sharply between two cases:

(i) char $\mathbb{F}$ does not divide $|G|$ (the *nonmodular* case);
(ii) char $\mathbb{F}$ divides $|G|$ (the *modular* case).

The latter case amounts to asserting that char $\mathbb{F} = p > 0$, and p divides $|G|$. This basic distinction between modular and nonmodular quickly appears when we study the invariant theory of pseudo-reflection groups. As we shall see, the nonmodular case is much easier to handle. Notably, given a finite subgroup $G \subset \mathrm{GL}(V)$, we can define the averaging operator

$$\mathrm{Av}\colon V \to V$$

$$\mathrm{Av}(x) = \frac{1}{|G|}\sum_{\varphi\in G} \varphi \cdot x.$$

It is a projection operator whose image consists of the invariants of G. In other words:

Lemma

(i) $(\mathrm{Av})^2 = \mathrm{Av}$;
(ii) $\mathrm{Im}\,\mathrm{Av} = V^G = \{x \in V \mid \varphi\cdot x = x \textit{ for all } \varphi \in G\}$.

Proof To prove (i) and (ii), it suffices, in turn, to show

(iii) $\mathrm{Av}(x) = x$ for all $x \in V^G$;
(iv) $\mathrm{Av}(x) \in V^G$ for all $x \in V$.

Regarding (iii), we have, for all $x \in V^G$, the equalities

$$\mathrm{Av}(x) = \frac{1}{|G|}\sum_{\varphi\in G} \varphi \cdot x = \frac{1}{|G|}\sum_{\varphi\in G} x = x.$$

Regarding (iv), we have, for all $x \in V$ and $\phi \in G$, the equalities

$$\phi \cdot \mathrm{Av}(x) = \frac{1}{|G|} \sum_{\varphi \in G} \phi\varphi \cdot x = \frac{1}{|G|} \sum_{\varphi \in G} \varphi \cdot x = \mathrm{Av}(x).$$

(The middle equality is obtained by *reindexing*.) ■

As an example of the usefulness of averaging, we cite Example 1 of §14-1. Again, the above averaging operator is used in Appendix B to prove Maschke's Theorem asserting the complete reducibility of representations in the nonmodular case. Maschke's theorem is used, in turn, in the proof of the proposition below.

The modular and nonmodular distinction can be applied to single linear maps $\varphi: V \to V$ of finite order. The nonmodular case occurs when $\operatorname{char} \mathbb{F}$ does not divide the order of φ, whereas the modular case occurs when $\operatorname{char} \mathbb{F}$ does divide the order of φ. In the rest of this section, we discuss pseudo-reflections in these two cases.

(a) Nonmodular Case In the nonmodular case, there is no difference between (generalized) reflections as discussed in §14-1 and pseudo-reflections. This follows from:

Proposition *If the order of a pseudo-reflection is finite and not divisible by* $\operatorname{char} \mathbb{F}$, *then it is diagonalizable.*

Proof We use Maschke's theorem from Appendix B. Let $s: V \to V$ be a pseudo-reflection with order not divisible by $\operatorname{char} \mathbb{F}$. Let G be the cyclic group generated by s. Then $\operatorname{char} \mathbb{F}$ does not divide $|G|$. The map $s: V \to V$ induces an action of G on V. Let H be the hyperplane left pointwise fixed by s and, hence, by G. By Maschke's theorem, we can find $\alpha \in V$ so that

$$V = H \oplus \mathbb{F}\alpha \quad \text{and} \quad \mathbb{F}\alpha \text{ is invariant under } s.$$

Clearly, α is an eigenvector and, so, we can diagonalize s. ■

(b) Modular Case Nondiagonalizable pseudo-reflections can occur in the modular case. However, other significant restrictions still occur in this case. Let us begin with fields of arbitrary characteristic. As already observed, a pseudo-reflection has a decomposition

$$s \cdot x = x + \Delta(x)\alpha,$$

and if we let

$$H = \operatorname{Ker} \Delta,$$

then s is nondiagonalizable if and only if $\alpha \in H$. If $\alpha \in H$ (i.e., $\Delta(\alpha) = 0$), it is easy to see that

$$s^k \cdot x = x + k\Delta(x)\alpha$$

for all $x \in V$. If we now assume that $\operatorname{char} \mathbb{F} = p$, then s must be of order p.

Almost all our discussion of invariant theory in subsequent chapters will involve the nonmodular case. Relatively little is known about the modular case. Modular invariant theory will only be discussed in Chapter 19.

To summarize this chapter, we have introduced, for every vector space, the concepts of "reflection" and "pseudo-reflection" and demonstrated that, most of the time, the two concepts are equivalent. It is only in the modular case that the two concepts can differ. In that case, a reflection is a special case of a pseudo-reflection. In the literature, the term "pseudo-reflection" is increasingly used in preference to the term "reflection". Throughout the rest of this book, we shall follow this convention. The concept of a pseudo-reflection will be used throughout the remainder of this book. It should be pointed out that, except in Chapter 19, we shall essentially be dealing only with the nonmodular case. So, except at that point, we could just as well have used "reflection". However, we prefer to follow common usage.

15 Classifications of pseudo-reflection groups

In this chapter, we sketch some of the classification results obtained for pseudo-reflection groups in the nonmodular case. The classification results given in this chapter are not used elsewhere, and are simply given as illustrations of the type of patterns that hold. We begin by sketching the Shephard-Todd classification of the finite complex pseudo-reflection groups. We then explain how this classification can be used to obtain classifications of pseudo-reflection groups over other fields. The Shephard-Todd classification is the key to all other classifications described in this chapter. We shall omit most details, and only sketch arguments.

15-1 Complex pseudo-reflection groups

The finite complex pseudo-reflection groups have no simple description akin to the Coxeter presentation for reflection groups in Euclidean space. Similarly, the classification of finite complex pseudo-reflection groups is a much more complicated affair than that given in Chapter 8 for the Euclidean case. The finite essential irreducible complex pseudo-reflection groups divide into 37 cases. They consist of three infinite families $\{\mathbb{Z}/m\mathbb{Z}\}$, $\{\Sigma_n\}$, $\{G(m,p,n)\}$, and 34 exceptional cases. The classification was first achieved by Shephard-Todd [1]. A more modern treatment is given in Cohen [1].

In dimension 1, we obviously must have $G = \mathbb{Z}/m\mathbb{Z}$. The classification argument for dimension ≥ 2 falls into three cases.

(a) Imprimitive Pseudo-Reflection Groups A group $G \subset \mathrm{GL}(V)$ is said to be *imprimitive* if there exists a decomposition $V = V_1 \oplus \cdots \oplus V_k$ $(k > 2)$, where the subspaces $\{V_i\}$ are permuted transitively by G. If $p|m$, we can define the semidirect group

$$G(m,p,n) = A(m,p,n) \rtimes \Sigma_n,$$

where

$$\Sigma_n = \text{the permutation matrices in } \mathrm{GL}_n(\mathbb{C})$$

$$A(m,p,n) = \left\{ \begin{bmatrix} \omega_1 & 0 & \cdots & 0 & 0 \\ 0 & \omega_{21} & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \omega_{n-1} & 0 \\ 0 & 0 & \cdots & 0 & \omega_n \end{bmatrix} \middle| \begin{array}{l} \omega_i^m = 1 \text{ and} \\ (\omega_1 \cdots \omega_n)^{m/p} = 1 \end{array} \right\}.$$

This group is an imprimitive pseudo-reflection group provided $n \geq 2$ because it acts on $V = \mathbb{C}^n$ by the rule that the factors of $\mathbb{C}^n$ are permuted by Σ_n and altered by scalars by $A(m,p,n)$. Observe that the construction includes many Euclidean

reflection groups as special cases:

$$G(2,1,n) = (\mathbb{Z}/m\mathbb{Z})^n \rtimes \Sigma_n = W(B_n) = W(C_n)$$
$$G(2,2,n) = (\mathbb{Z}/m\mathbb{Z})^{n-1} \rtimes \Sigma_n = W(D_n)$$
$$G(m,m,2) = \mathbb{Z}/m\mathbb{Z} \rtimes \Sigma_2 = D_m = G_2(m).$$

In all cases, $G(m,p,n)$ is a pseudo-reflection group. Notably, the involutions (i,j) in Σ_n are pseudo-reflections, as are the elements from $A(m,p,n)$, with only one entry of the form $\zeta \neq 1$ on the diagonal. We can show that the cases $n > 2$ of $G(m,p,n)$ give all irreducible imprimitive complex pseudo-reflection groups.

(b) Primitive Pseudo-Reflection Groups of Dimension 2 This case includes 19 exceptional pseudo-reflection groups. We want $G \subset \mathrm{GL}_2(\mathbb{C})$. We can decompose

$$\mathrm{GL}_2(\mathbb{C}) = \mathbb{C} \times \mathrm{SL}_2(\mathbb{C}),$$

where $\mathbb{C}$ denotes the scalar matrices $\left\{\left[\begin{smallmatrix}\lambda & 0\\ 0 & \lambda\end{smallmatrix}\right] \mid \lambda \in \mathbb{C}\right\}$. The conjugacy classes of finite subgroups of $\mathrm{SL}_2(\mathbb{C})$ are known. We have

$$\mathbb{Z}/m\mathbb{Z} = \left\langle \begin{bmatrix} e^{2\pi i/m} & 0 \\ 0 & e^{-2\pi i/m}\end{bmatrix} \right\rangle$$

$$D_m = \text{the dihedral group} = \left\langle \begin{bmatrix} i & 0 \\ 0 & i\end{bmatrix}, \begin{bmatrix} e^{2\pi i/m} & 0 \\ 0 & e^{-2\pi i/m}\end{bmatrix} \right\rangle$$

$$T = \text{the tetrahedral group} = \left\langle \left(\frac{1}{\sqrt{2}}\right) \begin{bmatrix} \varepsilon & \varepsilon^3 \\ \varepsilon & \varepsilon^7\end{bmatrix}, D_2 \right\rangle$$

$$O = \text{the octahedral group} = \left\langle \begin{bmatrix} \varepsilon^3 & 0 \\ 0 & \varepsilon^3\end{bmatrix}, T \right\rangle$$

$$I = \text{the icosahedral group}$$
$$= \left\langle \left(\frac{1}{\sqrt{5}}\right) \begin{bmatrix} \eta^4 - \eta & \eta^2 - \eta^3 \\ \eta^2 - \eta^3 & \eta - \eta^4\end{bmatrix}, \left(\frac{1}{\sqrt{5}}\right) \begin{bmatrix} \eta^2 - \eta^4 & \eta^4 - 1 \\ 1 - \eta & \eta^3 - \eta\end{bmatrix} \right\rangle.$$

The last three are the cases $k = 3, 4, 5$ of the group $\langle x, y \mid x^2 = y^3 = (xy)^k = 1\rangle$. These three groups have order 24, 48, 120, respectively. Given subgroups

$$H \lhd K \subset \mathrm{SL}_2(\mathbb{C}),$$

where

$$K/H = \mathbb{Z}/m\mathbb{Z},$$

we can define, for each $k > 1$, a group

$$G \subset \mathbb{Z}/km\mathbb{Z} \times K \subset \mathrm{GL}_2(\mathbb{C})$$

as the *pullback* in the diagram

$$\begin{array}{ccc} G & \longrightarrow & K \\ \downarrow & & \downarrow \\ \mathbb{Z}/km\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z}. \end{array}$$

G consists of all pairs (x, y) in $\mathbb{Z}/km\mathbb{Z} \times K$ such that x and y have the same image in $\mathbb{Z}/m\mathbb{Z}$. In particular, the bottom map is surjective and G fits into an *extension*

$$1 \to \mathbb{Z}/k\mathbb{Z} \to G \to K \to 1,$$

i.e., $\mathbb{Z}/k\mathbb{Z} \lhd G$ and $K =$ the quotient group $G/(\mathbb{Z}/k\mathbb{Z})$. All the subgroups of $GL_2(\mathbb{C})$ arise in this manner. Moreover, 19 of these cases give finite primitive pseudo-reflection groups. The cases $K = T, O$ and I give rise to 4, 8 and 7 pseudo-reflection groups, respectively.

(c) Primitive Pseudo-Reflection Groups of Dimension ≥ 3 This case is handled by techniques similar to those employed in the real case. We describe the irreducible pseudo-reflection groups by root graphs (or, in one case, by what is called a neat extension of a root graph).

Root Graphs The vertices consist of n linearly independent vectors $\{\alpha_1, \dots, \alpha_n\}$ in $\mathbb{C}^n$, with the property that $(\alpha_i, \alpha_j) = 1$ if and only if $\alpha_i = \alpha_j$. There is an edge between α_i and α_j, provided $(\alpha_i, \alpha_j) \neq 0$. Both vertices and edges are labelled. The vertex α_i is labelled by an integer $w(\alpha_i) \geq 2$. The edges between α_i and α_j are labelled by the numbers (α_i, α_j).

We can associate a pseudo-reflection group to each such graph. Given $0 \neq \alpha \in \mathbb{C}^n$ and an integer $k \geq 2$, define

$$s_{\alpha,k} \cdot x = x + (\xi_k - 1)\frac{(x, \alpha)}{(\alpha, \alpha)}\alpha,$$

where ξ_k is a primitive k-th root of unity. Since

$$s_{\alpha,k} \cdot \alpha = \xi_k \alpha \quad \text{and} \quad s_{\alpha,k} = 1 \text{ on the hyperplane } H_\alpha = \{x \mid (x, \alpha) = 0\},$$

we see that $s_{\alpha,k}$ is a pseudo-reflection of order k. Given a root graph with vertices $\{\alpha_i\}$, we associate with it the pseudo-reflection group generated by $\{s_{\alpha_i, w(\alpha_i)}\}$.

Conversely, every primitive irreducible pseudo-reflection group of dimension ≥ 3 (with the one exception already identified) can be produced by such a root graph. The resulting classification produces one infinite family $\{\Sigma_n\}$ and 15 exceptional cases.

We should note that the Coxeter graphs and their corresponding groups fit into the above pattern. Every Coxeter graph can be converted into a graph of the above type. To make the transition, label each vertice by "2" and label an edge by

"$-\cos(\frac{\pi}{m})$", rather than "m". For example, the Coxeter graph and the root graph of $D_m = G_2(m)$ are

$$\overset{}{\circ}\overset{m}{\text{———}}\circ \quad \text{and} \quad \overset{2}{\circ}\overset{-\cos\left(\frac{\pi}{m}\right)}{\text{—————————}}\overset{2}{\circ}$$

respectively.

Not all complex pseudo-reflection groups can be treated in terms of root graphs. The obstruction is that root graphs only produce n-dimensional pseudo-reflection groups generated by n pseudo-reflections. Some n-dimensional complex pseudo-reflection groups require $n+1$ pseudo-reflections to generate them. For example, $G(m,p,n)$ is generated by n pseudo-reflections only when $p = 1$ or $p = m$, i.e., only for $G(m,m,n)$ and $G(m,1,n)$. A complete list of n-dimensional pseudo-reflection groups generated by n pseudo-reflections is given in §11 of Shephard-Todd [1]. Pseudo-reflection groups with this property will be studied in §24-3.

Table 8 at the end of this chapter lists Shephard and Todd's results for the 37 types of finite essential irreducible complex pseudo-reflection groups.

15-2 Other pseudo-reflection groups in characteristic 0

Let $\mathbb{F}$ be a field of characteristic 0. Then the classification of finite essential irreducible pseudo-reflection groups defined over $\mathbb{F}$ can be obtained as a refinement of the Shephard-Todd classification of complex pseudo-reflection groups achieved in §15-1. To explain this, we need to work in the context of representation theory, as outlined in Appendix B.

First of all, pseudo-reflection groups defined over $\mathbb{F}$ are always complex pseudo-reflection groups. Suppose G is a $\mathbb{F}$ pseudo-reflection group by the representation

$$\rho\colon G \longrightarrow GL_n(\mathbb{F}).$$

Let $\mathbb{L}$ be a common extension of $\mathbb{F}$ and $\mathbb{C}$. Then ρ is obviously defined over $\mathbb{L}$. By a result of Brauer cited in Appendix B, ρ is defined over any subfield of $\mathbb{L}$ containing the $|G|$-th roots of unity. In particular, ρ is defined over $\mathbb{C} \subset \mathbb{L}$.

However, a given complex pseudo-reflection group is not necessarily a $\mathbb{F}$ pseudo-reflection group. The key obstruction is the character field of the representation. Recall, from Appendix B, that for a representation $\rho\colon G \longrightarrow GL_n(\mathbb{C})$ with character $\chi\colon G \longrightarrow \mathbb{C}^*$, the *character field* is given by

$$\mathbb{Q}(\chi) = \text{the extension of } \mathbb{Q} \text{ generated by } \operatorname{Im}\chi \subset \mathbb{C}^*.$$

In order to have $\rho\colon G \longrightarrow GL_n(\mathbb{C})$ defined over K, we must have $\mathbb{Q}(\chi) \subset K$. This condition is usually not sufficient. An arbitrary representation $\rho\colon G \longrightarrow GL_n(\mathbb{C})$ with character χ is usually not defined over $\mathbb{Q}(\chi)$ itself, only over a finite extension of $\mathbb{Q}(\chi)$. But, as explained in Appendix B, if ρ is an irreducible representation, and $\rho(G) \subset GL_n(\mathbb{C})$ contains a pseudo-reflection, then ρ is defined over $\mathbb{Q}(\chi)$. So a pseudo-reflection representation ρ is defined over $\mathbb{K}$ if and only if $\mathbb{Q}(\chi) \subset \mathbb{K}$,

where $\chi\colon G \to \mathbb{C}$ is the character of the chosen pseudo-reflection group. The above discussion gives the following equivalence.

***Theorem* (Clark-Ewing)** *Let G be a finite group. Then G has a representation as a (essential, irreducible) $\mathbb{F}$ pseudo-reflection group if and only if*

(i) G has a representation $\rho\colon G \to \mathrm{GL}_n(\mathbb{C})$ as a (essential, irreducible) complex pseudo-reflection group;
(ii) $\mathbb{Q}(\chi) \subset \mathbb{F}$, where χ is the character of ρ.

We now have a program for classifying $\mathbb{F}$ pseudo-reflection groups. Take each of the 37 finite essential irreducible complex pseudo-reflection groups in the Shephard-Todd list and determine when one has $\mathbb{Q}(\chi) \subset \mathbb{F}$. A case-by-case study of the complex pseudo-reflection groups yields that, in every case, $\mathbb{Q}(\chi)$ is an extension of $\mathbb{Q}$ involving

$$\xi_n = e^{\frac{2\pi i}{n}}, \xi_n + \xi_{-n}, \sqrt{2}, \sqrt{-2}, \sqrt{5} \text{ and } \sqrt{-7}.$$

So it becomes a matter of determining when these elements belong to $\mathbb{F}$. This programme was carried out by Clark-Ewing [1] in the case of p-adic pseudo-reflection groups.

15-3 Pseudo-reflection groups in characteristic p

To date, no one has obtained a classification for pseudo-reflection groups in characteristic p analogous to those described in §15-1 and §15-2 for characteristic 0. However, some restrictions can be obtained. We shall sketch the arguments.

We can find a local ring R (actually a discrete valuation ring) such that $R/m = \mathbb{F}$ where m is the unique maximal ideal of R. If $\mathbb{F}$ is perfect, we can use the Witt vector construction on $\mathbb{F}$ to obtain R. In the general case (see Schoeller [1]), R is a subring of the Witt vectors. Let $\mathcal{F}$ be the fraction field of R. Then $\mathcal{F}$ is of characteristic 0. Hence, by the results of §15-2, we can assume that the pseudo-reflection groups are known. The following result then determines the $\mathbb{F}$ pseudo-reflection groups in the nonmodular case.

Theorem *Let G be a finite group of order prime to p. Then G has a representation as a (essential irreducible) $\mathbb{F}$ pseudo-reflection group if and only if G has a representation as a (essential irreducible) $\mathcal{F}$ pseudo-reflection group.*

The correspondence is established by using R representations. Let G have order prime to p. We show that, given a representation $\rho\colon G \to \mathrm{GL}_n(\mathbb{F})$, there exists a representation $\widehat{\rho}\colon G \to \mathrm{GL}_n(R)$ inducing ρ. In turn, $\widehat{\rho}$ induces a $\mathcal{F}$ representation. This construction sends $\mathbb{F}$ pseudo-reflection representations to $\mathcal{F}$ pseudo-reflection representations. Verifying this fact demands some results from invariant theory, notably, that a pseudo-reflection group is characterized by its ring of invariants being a polynomial algebra (see Chapter 18 for this result). We obtain, in this manner, a one-to-one correspondence between representations of G as a $\mathbb{F}$ pseudo-reflection group and representations of G as a $\mathcal{F}$ pseudo-reflection group.

Number	Rank	Order	Character Field	Degrees
1	n	$(n+1)!$	$\mathbb{Q}$	$2, 3, \ldots, n+1$
$2a$	n	$qm^{n-1}n!$	$\mathbb{Q}(\xi)$	$m, m+1, \ldots, (n-1)m, qn$
$2b$	2	$2m$	$\mathbb{Q}(\xi+\xi^{-1})$	$2, m$
3	1	m	$\mathbb{Q}(\xi)$	m
4	2	24	$\mathbb{Q}(\omega)$	$4, 6$
5	2	72	$\mathbb{Q}(\iota)$	$6, 12$
6	2	48	$\mathbb{Q}(\iota, \omega)$	$4, 12$
7	2	144	$\mathbb{Q}(\iota, \omega)$	$12, 12$
8	2	96	$\mathbb{Q}(\iota)$	$8, 12$
9	2	192	$\mathbb{Q}(\iota, \sqrt{2})$	$8, 24$
10	2	288	$\mathbb{Q}(\iota, \omega)$	$12, 24$
11	2	576	$\mathbb{Q}(\epsilon, \omega)$	$24, 24$
12	2	48	$\mathbb{Q}(\sqrt{}-2)$	$6, 8$
13	2	96	$\mathbb{Q}(\iota, \sqrt{2})$	$8, 12$
14	2	144	$\mathbb{Q}(i, \omega)$	$6, 24$
15	2	288	$\mathbb{Q}(\iota, \omega, \sqrt{2})$	$12, 24$
16	2	600	$\mathbb{Q}(\eta)$	$20, 30$
17	2	1200	$\mathbb{Q}(\iota, \eta)$	$20, 60$
18	2	1800	$\mathbb{Q}(\omega, \eta)$	$30, 60$
19	2	3600	$\mathbb{Q}(\omega, \iota, \eta)$	$60, 60$
20	2	360	$\mathbb{Q}(\omega, \sqrt{5})$	$12, 30$
21	2	720	$\mathbb{Q}(\iota, \omega, \sqrt{5})$	$12, 60$
22	2	240	$\mathbb{Q}(\iota, \sqrt{5})$	$12, 20$
23	3	120	$\mathbb{Q}(\sqrt{5})$	$2, 6, 10$
24	3	336	$\mathbb{Q}(\sqrt{}-7)$	$4, 6, 14$
25	3	648	$\mathbb{Q}(\omega)$	$6, 9, 12$
26	3	1296	$\mathbb{Q}(\omega)$	$6, 12, 18$
27	3	2160	$\mathbb{Q}(\omega, \sqrt{5})$	$6, 12, 30$
28	4	1152	$\mathbb{Q}$	$2, 6, 8, 12$
29	4	7680	$\mathbb{Q}(\iota)$	$4, 8, 12, 20$
30	4	14,400	$\mathbb{Q}(\sqrt{5})$	$2, 12, 20, 30$
31	4	$64 \cdot 6!$	$\mathbb{Q}(\iota)$	$8, 12, 20, 24$
32	4	$216 \cdot 6!$	$\mathbb{Q}(\omega)$	$12, 18, 24, 30$
33	5	$72 \cdot 6!$	$\mathbb{Q}(\omega)$	$4, 6, 10, 12, 18$
34	6	$108 \cdot 9!$	$\mathbb{Q}(\omega)$	$6, 12, 18, 24, 30, 42$
35	6	$72 \cdot 6!$	$\mathbb{Q}$	$2, 5, 6, 8, 9, 12$
36	7	$8 \cdot 9!$	$\mathbb{Q}$	$2, 6, 8, 10, 12, 14, 18$
37	8	$192 \cdot 10!$	$\mathbb{Q}$	$2, 8, 12, 14, 18, 20, 24, 30$

Table 8: Complex pseudo-reflection groups

The above only applies to the nonmodular case, i.e., when p does not divide $|G|$. There is very little known about the modular case, i.e., when p divides $|G|$. Certainly, the $\mathcal{F}$ pseudo-reflection groups do not give the answer.

Table 8 contains the Shephard and Todd classification of the 37 types of finite essential irreducible complex pseudo-reflection groups. Degrees of pseudo-reflection groups (which appear in the last column) were introduced in § 1-7 and will reappear in §18-1. Regarding degrees, the Euclidean reflection groups are distinguished on this list by the fact that they have 2 as one of their degrees. A theoretical justification of this observation will be given in §18-6. In the chart,

$$\zeta = e^{\frac{2\pi}{m}i} = \sqrt{-1}, \quad \omega = e^{\frac{2\pi i}{3}}, \quad \eta = e^{\frac{2\pi i}{5}}, \quad \epsilon = e^{\frac{2\pi i}{8}}.$$

Moreover, in case $2a$, p, q and m are related by the rule $pq = m$.

V Rings of invariants

Part V constitutes a basic introduction to invariant theory. The invariant ring of a finite group is introduced and its properties are studied, in particular the invariant ring of pseudo-reflection groups. In Chapter 16, we introduce rings of invariants and demonstrate that they are finitely generated, and usually satisfy the Cohen-Macauley property. In Chapter 17, we introduce Poincaré series and demonstrate how they can be used to analyze rings of invariants. Notably, we prove Molien's theorem establishing a relation between the eigenvalues of $G \subset \mathrm{GL}(V)$ and the Poincaré series of the ring of invariants of G. In Chapter 18, we demonstrate that pseudo-reflection groups are canonical objects to consider from the perspective of invariant theory. We prove that, in the nonmodular case, a pseudo-reflection group is characterized by the property that its ring of invariants is polynomial. In Chapter 19, we demonstrate that, in the modular case, only pseudo-reflection groups have polynomial rings of invariants.

16 The ring of invariants

In this chapter we introduce the ring of invariants of a finite group and examine some of its basic properties. These properties include Galois properties, the Noetherian property and the Cohen-Macauley property. We note that an initial discussion of ring of invariants took place in §1-7.

16-1 The ring of invariants

Let $\mathbb{F}$ be any field and let V be a finite dimensional $\mathbb{F}$ vector space. Given any group $G \subset \mathrm{GL}(V)$, we can form its associated ring of invariants. First, we form the tensor algebra

$$T(V) = \bigoplus_{j=0}^{\infty} V^{\otimes j} = \mathbb{F} \oplus V \oplus (V \otimes V) \oplus \cdots .$$

There is an obvious tensor product on $T(V)$. Given $x = x_1 \otimes \cdots \otimes x_s \in V^{\otimes s}$ and $y = y_1 \otimes \cdots \otimes y_t \in V^{\otimes t}$, we can form the product

$$x \otimes y = x_1 \otimes \cdots \otimes x_s \otimes y_1 \otimes \cdots \otimes y_t \in V^{\otimes (s+t)}.$$

This tensor product gives $T(V)$ the structure of a noncommutative, associative $\mathbb{F}$ algebra.

A basic introduction to graded rings and modules is provided in Appendix A. An $\mathbb{F}$ algebra A is *graded* if it has a decomposition $A = \bigoplus_{j=0}^{\infty} A_j$, where each A_i is an $\mathbb{F}$ vector space and the multiplication $A \otimes A \longrightarrow A$ is compatible with the decomposition, in that it induces maps $A_i \otimes A_j \longrightarrow A_{i+j}$. The elements of A_i are said to be *homogeneous* elements of *degree* i. The compatibility of the multiplication with the grading can be restated as asserting that $\deg x = i$ and $\deg y = j$ forces $\deg xy = i + j$. The algebra $T(V)$ is graded by means of the above decomposition $T(V) = \bigoplus_{j=0}^{\infty} V^{\otimes j}$ with the elements of $V^{\otimes j}$ being the homogeneous elements of degree j.

Given a graded associative algebra $A = \bigoplus_{j=0}^{\infty} A_j$, an ideal $I \subset A$ is *graded* if it admits a decomposition $I = \bigoplus_{j=0}^{\infty} I_j$, where $I_j = I \cap A_j$. A graded ideal is generated by homogeneous elements. (For example, the ideal of $\mathbb{F}[t]$ generated by $t + t^2$ is not graded.) Given a (two-sided) graded ideal $I \subset A$, then the quotient algebra A/I inherits a grading from A.

The *symmetric algebra* $S(V)$ is such a quotient algebra. To define $S(V)$, choose the graded ideal $I \subset T(V)$ generated by $\{x \otimes y - y \otimes x \mid x, y \in V\}$ and let

$$S(V) = T(V)/I.$$

The effect of quotienting out by I is to make the tensor product commutative. So $S(V)$ is a commutative associative graded algebra

$$S(V) = \bigoplus_{j=0}^{\infty} S_j(V).$$

$S(V)$ is a free algebra generated by any basis of $S_1(V) = V$. More exactly, if $\{t_1, \ldots, t_n\}$ is a basis of V, then every element in $S(V)$ can be written uniquely as a polynomial in $\{t_1, \ldots, t_n\}$. We shall write

$$S(V) = \mathbb{F}[t_1, \ldots, t_n]$$

and call $S(V)$ a *polynomial algebra.* The elements $\{t_1, \ldots, t_n\}$ have degree 1. This notation and terminology was introduced in §1-7. It originates from the case where we replace V by its dual vector space V^*. If $\mathbb{F}$ is an infinite field, we can think of $S(V^*)$ as the polynomial functions $f\colon V \to \mathbb{F}$. Under this identity, addition and multiplication in $S(V^*)$ correspond to the usual operations for polynomials. Also, the grading in $S(V^*)$ corresponds to the grading for polynomials given by the degree of a polynomial.

We also remark that, as in §1-7, we shall find it useful to expand the use of the polynomial algebra notation, $\mathbb{F}[x_1, \ldots, x_n]$, to include the cases where the generators $\{x_1, \ldots, x_n\}$ have arbitrary degree. This notation will be used in future discussions (e.g., the examples in §16-2).

Given a group $G \subset \mathrm{GL}(V)$, then the action of G on V induces an action on $S(V)$. We extend the action of G on V to all of $S(V)$ by the multiplicative rule

$$\varphi \cdot (x_1 x_2 \cdots x_n) = (\varphi \cdot x_1)(\varphi \cdot x_2) \cdots (\varphi \cdot x_n)$$

for any $\varphi \in G$. We then define the *ring of invariants*

$$S(V)^G = \{f \in S(V) \mid \varphi \cdot f = f \text{ for all } \varphi \in G\}.$$

The action of G on $S(V)$ respects its grading. So $S(V)^G$ inherits a grading from $S(V)$.

$$S(V)^G = \bigoplus_{j=0}^{\infty} S_i(V)^G.$$

Besides looking at the invariants of $S(V)$, we can also look at the invariants of $S(V^*)$, where V^* is the dual vector space of V. The action of G on V induces an action on V^* by the rule

$$\langle \varphi \cdot \alpha, y \rangle = \langle \alpha, \varphi^{-1} \cdot y \rangle$$

for any $\alpha \in V^*$, $y \in V$ and $\varphi \in G$. The action of G on V^* extends to an action on $S(V^*)$, and we can consider $S(V^*)^G$.

There is significant interest in the invariants $S(V^*)^G$. Generally, they are the same as the set of G-invariant polynomial functions on V because, as already remarked, when $\mathbb{F}$ is infinite, we can identify $S(V^*)$ with the polynomial functions on V. And, under this identity, the above action of G on $S(V^*)$ corresponds to the action of G on the polynomial functions given by

$$\varphi \cdot f(x) = f(\varphi^{-1} \cdot x)$$

for any $x \in V$ and $\varphi \in G$.

Historically, invariant polynomials have been the major subject of invariant theory, and there will be times when we shall want to deal with $S(V^*)$ rather than $S(V)$, mainly for the above-mentioned reason that $S(V^*)$ can be interpreted as the polynomial functions on V. Nevertheless, we shall generally establish results for $S(V)$ and $S(V)^G$, rather than $S(V^*)$ and $S(V^*)^G$. The results proved for $S(V)^G$ hold for $S(V^*)^G$ as well, with only the occasional minor modification. We shall identify such modifications when they occur. The advantage in working with $S(V)$ rather than $S(V^*)$ is that we can sometimes simplify arguments. Notably, we avoid having to constantly dualize the action of G.

16-2 Examples

In this section, we present a few simple examples of rings of invariants. We consider groups obviously motivated by the A_n, B_n, D_n cases of finite Euclidean reflection groups considered in §2-2. Notably, the first two examples are straightforward generalizations of the invariant rings considered in §1-7.

Example 1: Let $G = \Sigma_n$, the permutation group, let V be an n-dimensional vector space over the field $\mathbb{F}$, and let Σ_n act on V by permuting a chosen basis of V. If $\{t_1, \ldots, t_n\}$ is the chosen basis of V, we can write

$$S(V) = \mathbb{F}[t_1, \ldots, t_n],$$

with $G = \Sigma_n$ acting on $S(V)$ by permuting $\{t_1, \ldots, t_n\}$. Thus $S(V)^G =$ the symmetric polynomials in $\{t_1, \ldots, t_n\}$. These symmetric polynomials have been extensively studied. We can write

$$S(V)^G = \mathbb{F}[s_1, \ldots, s_n],$$

where s_k is the k-th *elementary symmetric polynomial* given by

$$s_k = \sum_{1 \leq i_1 < \cdots < i_k \leq n} t_{i_1} \cdots t_{i_k} = \text{the coefficient of } T^{n-k} \text{ in } \prod_{i=1}^{k} (T + t_i).$$

Example 2: Let $G = (\mathbb{Z}/2\mathbb{Z})^n \rtimes \Sigma_n$ act on an n-dimensional vector space V by the rule that Σ_n permutes a chosen basis, whereas $(\mathbb{Z}/2\mathbb{Z})^n$ changes the signs of these basis elements. Write

$$S(V) = \mathbb{F}[t_1, \ldots, t_n],$$

where $\{t_1, \ldots, t_n\}$ is this chosen basis of V. If $\operatorname{char} \mathbb{F} = 2$, we can ignore $(\mathbb{Z}/2\mathbb{Z})^n$ and we get the same answer as in Example 1. If $\operatorname{char} \mathbb{F} \neq 2$, then

$$S(V)^G = \mathbb{F}[\tilde{s}_1, \ldots, \tilde{s}_n],$$

where

$$\tilde{s}_k = \sum_{1 \le i_1 < \cdots < i_k \le n} t_{i_1}^2 \cdots t_{i_k}^2.$$

Example 3: Let $G = (\mathbb{Z}/2\mathbb{Z})^{n-1} \rtimes \Sigma_n$ act on an n-dimensional vector space by the rule that Σ_n permutes a chosen basis, whereas $(\mathbb{Z}/2\mathbb{Z})^{n-1}$ consists of the elements changing the sign on an even number of basis elements. If we write $S(V) = \mathbb{F}[t_1, \ldots, t_n]$, where $\{t_1, \ldots, t_n\}$ is the chosen basis of V, then for char $\mathbb{F} \neq 2$

$$S(V)^G = \mathbb{F}[\tilde{s}_1, \ldots, \tilde{s}_{n-1}, t],$$

where $\tilde{s}_k$ is as above and

$$t = t_1 t_2 \cdots t_n.$$

In the above examples, the ring of invariants are very simple, which is atypical. The structure of $S(V)^G$ can be quite complicated. As already mentioned, the groups chosen above are extensions to arbitrary fields of finite Euclidean reflection groups. In particular, they are pseudo-reflection groups. The fact that the invariants of these groups turn out to be polynomial algebras is not accidental. In Chapter 18, we shall prove that, under a nonmodular hypothesis, the invariants of a finite pseudo-reflection group always form a polynomial algebra. In Chapter 19, we shall prove, without any hypothesis, the converse relation: that the invariants of a finite group being polynomial force the group to be a pseudo-reflection group.

16-3 Extension theory

In our subsequent study of invariant theory, we shall be using graded analogues of classical field and ring theory. This section is an introduction to these ideas. We note that graded rings and algebras are discussed in Appendix A and in §16-1.

Let V be a finite dimensional $\mathbb{F}$ vector space and let $G \subset \mathrm{GL}(V)$ be a finite group. Throughout this section, we shall work in the context of *graded* $\mathbb{F}$ *integral domains*, namely graded $\mathbb{F}$ vector spaces $H = \bigoplus_{j \in \mathbb{Z}}^{\infty} H_i$ with multiplications $H_i \otimes_{\mathbb{F}} H_j \to H_{i+j}$ inducing an integral domain structure on H. In particular $S(V)^G$ and $S(V)$ are such objects. Our goal in introducing the theory of graded integral domains is to provide a context for studying the extension $S(V)^G \subset S(V)$.

We begin by introducing some standard definitions about extensions in the context of graded $\mathbb{F}$ integral domains. We point out that, given a graded $\mathbb{F}$ integral domain H, we can make the polynomial ring $H[X]$ a graded $\mathbb{F}$ integral domain by assigning a degree to the variable X. Given an embedding $H \subset K$, then $x \in K^d$ is *algebraic* over H if $f(x) = 0$ for some homogeneous polynomial $f(X) \in H[X]$, where the variable is assumed to have degree d. We say K is an *algebraic extension* of H if every element of K is algebraic over H. Given $H \subset K$, if $x \in K$ is algebraic, then the monic polynomial $f(X) \in H[X]$ of smallest degree such that $f(x) = 0$ is called the *minimal polynomial* of x. The *transcendence degree* of K is the maximal

number of algebraically independent elements in K (over $\mathbb{F}$). The element $x \in K$ is *integral* over H if there exists a monic homogeneous polynomial

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \quad (a_i \in A),$$

where $f(x) = 0$. If every element of K is integral over H, we say that K is integral over H.

Proposition A *If $G \subset \mathrm{GL}(V)$ is finite, then $S(V)$ is integral over $S(V)^G$.*

Proof Given $x \in S(V)$, let

$$f(t) = \prod_{\varphi \in G} (T - \varphi \cdot x).$$

Then $f(x) = 0$. Also, this polynomial is of the form $f(T) = T^k + a_{k-1}T^{k-1} + \cdots + a_1T + a_0$, where $a_i \in S(V)^G$ because all the coefficients (except the leading one) are elementary symmetric polynomials in $\{\varphi \cdot x\}_{\varphi \in G}$. Since the elements of G permute the elements $\{\varphi \cdot x\}_{\varphi \in G}$, it follows that these elementary symmetric polynomials are invariant under the action of G and, hence, belong to $S(V)^G$. ■

We are particularly concerned with Galois properties. An extension $H \subset K$ is *finite* if K is a finitely generated H module. A finite extension $H \subset K$ is *Galois* if $H = K^G$, where G is the group of automorphisms of K fixing H. G is called the *Galois group* of the extension. In general, we have an inclusion, $H \subset K^G$, but not equality. Every Galois extension satisfies the properties of normality and separability. Conversely, in the case of an algebraic extension $H \subset K$, these properties force the equality $H = K^G$. An extension $H \subset K$ is *normal* if, for any homogeneous polynomial $f(X) \in H[X]$, the presence in K of one root of $f(X)$ forces $f(X)$ to split in $K[X]$ into linear factors. An algebraic extension is *separable* if, for every $x \in K$, the minimal polynomial $f(x) = 0$ also satisfies $f'(x) \neq 0$. $H \subset K$ is a *splitting domain* for the polynomial $f(X) \in H[X]$ if K is the smallest extension of H containing all the roots of $f(X)$. A splitting domain is always normal.

We can apply the next proposition to the inclusion $S(V)^G \subset S(V)$ and conclude that it is a finite extension because $S(V) = \mathbb{F}[t_1, \ldots, t_n]$ is finitely generated and, by Proposition A, $S(V)^G \subset S(V)$ is integral.

Proposition B *Given an inclusion $A \subset B$, where B is integral over A and also finitely generated as an A algebra, then B is finite over A.*

Proof Choose $\{\alpha_1, \ldots, \alpha_n\}$, which generate B as an A algebra. We have the series of extensions

$$A \subset A[\alpha_1] \subset A[\alpha_1, \alpha_2] \subset \cdots \subset A[\alpha_1, \ldots, \alpha_n] = B,$$

where $A[\alpha_1, \ldots, \alpha_k]$ denotes the subalgebra of B generated by A and $\{\alpha_1, \ldots, \alpha_k\}$. Since each α_i is integral, it follows that each extension is finite. Consequently, B is finite over A. ■

The above discussion of Galois theory also applies to the extensions $F(H) \subset F(K)$ of fraction fields. In fact, this is where the most natural analogues of classical Galois theory occur.

16-4 Properties of rings of invariants

Although rings of invariants can be complicated, they still possess some reasonable structure. In this section, we prove that rings of invariants are Noetherian and typically Cohen-Macauley. As before, V is any finite dimensional vector space over $\mathbb{F}$, and $G \subset \mathrm{GL}(V)$ is any group. We shall prove:

***Theorem A* (Hilbert-Noether)** *If $G \subset \mathrm{GL}(V)$ is finite, then $S(V)^G$ is a finitely generated $\mathbb{F}$ algebra.*

Proof Our method will be to locate a finitely generated algebra $A \subset S(V)^G$ so that the extension is finite. It follows that $S(V)^G$ must also be finitely generated.

First of all, we define A. We have already observed in §16-3 that $S(V)$ is integral and finite over $S(V)^G$. We let A be the algebra generated by the coefficients of the (finitely many!) polynomials used to show $S(V)$ is integral over $S(V)^G$.

Secondly, the extension $A \subset S(V)^G$ is finite. It suffices to show $A \subset S(V)$ is finite because, since A is Noetherian, any submodule of a finitely generated A module is also finitely generated. By definition, $S(V)$ is integral over A. Also, $S(V)$ is finitely generated. So we can apply Proposition 16-3B to show that $A \subset S(V)$ is finite. ■

We next prove that the ring of invariants for finite $G \subset \mathrm{GL}(V)$ often possesses the pleasant property of being Cohen-Macauley.

Definition: A ring A is a *Cohen-Macauley (CM)* if there exists a polynomial subalgebra $\mathbb{F}[x_1, \ldots, x_n] \subset A$ such that A is free and finite over $\mathbb{F}[x_1, \ldots, x_n]$. In other words, we can choose $\{\alpha_1, \ldots, \alpha_s\} \subset A$ so that

$$A = \bigoplus_{i=1}^{s} \mathbb{F}[x_1, \ldots, x_n]\alpha_i.$$

Remark: The CM property is basically concerned with the freeness property. First of all, observe that the CM property forces A to be finitely generated. So we might as well only consider finitely generated algebras. Secondly, given any finitely generated A that is an integral domain, we can choose $\mathbb{F}[x_1, \ldots, x_n] \subset A$ such that A is integral over $\mathbb{F}[x_1, \ldots, x_n]$. This is the Noether Normalization Theorem (see §4 of Chapter X of Lang [1]). Thirdly, it follows from Proposition 16-2B that A is finite over $\mathbb{F}[x_1, \ldots, x_n]$. So only the freeness property is in question.

The polynomial generators $\{x_1, \ldots, x_n\}$ given by the Noether Normalization Theorem are called a *system of parameters* of A. Parameters are not unique. For example, we could replace $\mathbb{F}[x_1, \ldots, x_n] \subset A$ by $\mathbb{F}[x_1^{k_1}, \ldots, x_n^{k_n}]$. On the other hand, the number of parameters (= the *transcendence degree*) is unique. Regarding the question of freeness, if A is free over $\mathbb{F}[x_1, \ldots, x_n]$ for one system of parameters $\{x_1, \ldots, x_n\}$, then A is free over $\mathbb{F}[y_1, \ldots, y_n]$ for any system of parameters $\{y_1, \ldots, y_n\}$.

The rest of this section will be devoted to proving:

Theorem B **(Hochster-Eagan)** *If $G \subset \mathrm{GL}(V)$ is a finite nonmodular subgroup, then $S(V)^G$ is Cohen-Macauley.*

The proof involves the averaging operator

$$\mathrm{Av}\colon S(V) \to S(V)$$

$$\mathrm{Av}(x) = \frac{1}{|G|}\sum_{\varphi \in G} \varphi \cdot x.$$

As in §14-3, this operator satisfies a number of useful properties:

(i) Av is a projection operator onto $S(V)^G$, i.e., $(\mathrm{Av})^2 = \mathrm{Av}$ and $\mathrm{Im}\,\mathrm{Av} = S(V)^G$;
(ii) Av is a map of $S(V)^G$ modules, i.e.,

$$\mathrm{Av}(xy) = x\,\mathrm{Av}(y) \quad \text{for all } x \in S(V)^G, y \in S(V).$$

It follows from the above properties that we have a splitting:

(iii) $S(V) = S(V)^G \oplus \mathrm{Ker}\,\mathrm{Av}$ as $S(V)^G$ modules.

We can use the Noether Normalization Theorem to choose a polynomial algebra

$$\mathbb{F}[x_1, \ldots, x_n] \subset S(V)^G$$

such that $S(V)^G$ is finite over $\mathbb{F}[x_1, \ldots, x_n]$. The Cohen-Macauley property then follows from:

Lemma *Suppose $G \subset \mathrm{GL}(V)$ is a finite nonmodular subgroup. Given $\mathbb{F}[x_1, \ldots, x_n] \subset S(V)^G$, if $S(V)^G$ is finite over $\mathbb{F}[x_1, \ldots, x_n]$, then $S(V)^G$ is free over $\mathbb{F}[x_1, \ldots, x_n]$.*

Proof We first show that, when we consider $\mathbb{F}[x_1, \ldots, x_n] \subset S(V)$, then

$(*)$ $\qquad S(V)$ is free over $\mathbb{F}[x_1, \ldots, x_n]$.

We can write $S(V) = \mathbb{F}[t_1, \ldots, t_n]$. Thus $\{t_1, \ldots, t_n\}$ is a system of parameters for $S(V)$. Since $S(V)$ is free with respect to this system of parameters, it will be free with respect to any system of parameters. So to prove $(*)$, it suffices to show that $\{x_1, \ldots, x_n\}$ is a system of parameters for $S(V)$. Now, $S(V)$ is finite over $\mathbb{F}[x_1, \ldots, x_n]$. For, both of the inclusions

$$\mathbb{F}[x_1, \ldots, x_n] \subset S(V)^G \subset S(V)$$

are finite (to prove this for the second inclusion, we use the arguments from §16-3). Thus $\{x_1, \ldots, x_n\}$ is a system of parameters for $S(V)$.

By property (iii) of Av we can decompose

$(**)$ $\qquad S(V) = S(V)^G \oplus \mathrm{Ker}\,\mathrm{Av} \quad$ as $\mathbb{F}[x_1, \ldots, x_n]$ modules.

It follows from $(*)$ and $(**)$, and from the Proposition in Appendix A, that $S(V)^G$ (as well as Ker Av) is a free $\mathbb{F}[x_1, \ldots, x_n]$ module. ∎

16-5 The Dickson invariants

We produce in this section a more complicated example of a polynomial ring of invariants than those considered in §16-2. The group we shall consider is $GL(V)$, where V is a finite dimensional vector space, say of dimension n, over a field $\mathbb{F}$ of characteristic $p > 0$. So $|\mathbb{F}| = q = p^k$ for some $k \geq 1$ and $|V| = q^n$. The fact that $GL(V)$ is a pseudo-reflection group was observed in §14-2. The invariants of $GL(V)$ were studied in Dickson [1] and, as a result, are called the *Dickson invariants*. We shall follow the treatment of Dickson's argument as given in Wilkerson [1]. See also Steinberg [5].

Consider the polynomial

$$f(X) = \prod_{v \in V}(X - v) = f_0 + f_1 X + \cdots + f_{q^n} X^{q^n}$$

in $S(V)[X]$. The coefficients $\{f_1, \ldots, f_n\}$ are obtained by multiplying out the product $\prod_{v \in V}(X - v)$ and collecting terms according to the power of X involved. We have

$$f_i \in S(V)^{GL(V)}.$$

For, f_i is a symmetric polynomial in the nonzero elements of V, and these nonzero elements are permuted by each $\varphi \in GL(V)$. Consider, in particular, the coefficients

$$x_i = f_{q^n - q^{i-1}}.$$

In this section we shall prove:

***Theorem* (Dickson)** $S(V)^{GL(V)} = \mathbb{F}[x_1, \ldots, x_n]$.

We begin by comparing $f(X)$ to another polynomial. Let $\{t_1, \ldots, t_n\}$ be a basis of V. Consider the determinant

$$\Delta = \det \begin{bmatrix} t_1 & \cdots & t_n & X \\ t_1^q & \cdots & t_n^q & X^q \\ \vdots & & & \vdots \\ t_1^{q^n} & \cdots & t_n^{q^n} & X^{q^n} \end{bmatrix}.$$

Here we are working with coefficients in the polynomial ring $S(V)[X]$. If we expand Δ along the last column, then Δ is a polynomial of the form

$$\Delta(X) = \sum_{i=0}^{n} (-1)^{n-i} c_i X^{q^i}.$$

Next, we pass from $S(V)$ to

$$K = \text{the field of fractions of } S(V)$$

and work in $K[X]$. By using column operations, it is easy to see that

$$\Delta(v) = 0 \quad \text{for all } v \in V.$$

For, if we replace X by v in the above matrix, then the last column is a linear combination of the other columns. We use the same coefficients as used to write v as a linear combination of $\{t_1, \dots, t_n\}$. For, suppose that $v = c_1t_1 + \cdots + c_nt_n$, where $c_i \in \mathbb{F}$. Since $x^q = x$ for all $x \in \mathbb{F}$, it follows that $v^{q^i} = c_1(t_1)^{q^i} + \cdots + c_n(t_n)^{q^i}$ for each $0 \leq i \leq n$.

Thus $f(X)|\Delta(X)$ in $K[X]$. Since $f(X)$ and $\Delta(X)$ are polynomials of the same degree and $f(X)$ is monic, we must have

$$(*) \qquad \Delta(X) = c_n f(X).$$

Moreover,

$$(**) \qquad c_n = \det \begin{bmatrix} t_1 & \cdots & t_n \\ t_1^q & \cdots & t_n^q \\ \vdots & & \vdots \\ t_1^{q^{n-1}} & \cdots & t_n^{q^{n-1}} \end{bmatrix} \neq 0.$$

The equality in $(**)$ is true by definition. Regarding the inequality, it suffices to show

$$\det[t_j^{q^i}] = \prod(\alpha_1t_1 + \cdots + \alpha_nt_n),$$

where $(\alpha_1, \dots, \alpha_n)$ ranges through all nonzero tuples where the last nonzero α_i is 1. By column operations, we show that each $\alpha_1t_1 + \cdots + \alpha_nt_n$, and hence their product, divides $\det[t_j^{q^i}]$. Moreover, $\det[t_j^{q^i}]$ and $\prod(\alpha_1t_1 + \cdots + \alpha_nt_n)$ have the same degree and the monomial $t_1t_2^q \cdots t_{n-1}^{q^{n-1}}$ occurs in both with the same coefficient $(= 1)$. So they are equal. Now let

$$R = \text{the subalgebra of } S(V) \text{ generated over } \mathbb{F} \text{ by } \{x_1, \dots, x_n\}.$$

It follows from $(*)$ and $(**)$ that $f(X) \in R[X]$. Since all the elements of V are roots of $f(X)$, it follows that:

Lemma A *$S(V)$ is integral over R.*

Since $S(V)$ has transcendence degree n, it follows from Lemma A that R has transcendence degree n. Since R is generated by $\{x_1, \dots, x_n\}$, it follows that:

Corollary $R = \mathbb{F}[x_1, \dots, x_n]$.

We have $\mathbb{F}[x_1, \dots, x_n] \subset S(V)^{\mathrm{GL}(V)}$. Let

$$\mathbb{F}(x_1, \dots, x_n) = \text{the fraction field of } \mathbb{F}[x_1, \dots, x_n].$$

To prove $\mathbb{F}[x_1, \dots, x_n] = S(V)^{\mathrm{GL}(V)}$, it suffices to show $S(V)^{\mathrm{GL}(V)} \subset \mathbb{F}(x_1, \dots, x_n)$. For, by Lemma A, $S(V)^{\mathrm{GL}(V)}$ is integral over $\mathbb{F}[x_1, \dots, x_n]$. And, since $\mathbb{F}[x_1, \dots, x_n]$ is polynomial, it is integrally closed in its field of fractions. (Integral closure, in particular the fact that polynomial algebras are integrally closed, is discussed in part (b) of §19-1.)

To prove $S(V)^{\mathrm{GL}(V)} \subset \mathbb{F}(x_1, \dots, x_n)$, it clearly suffices to prove:

Lemma B $K^{\mathrm{GL}(V)} = \mathbb{F}(x_1, \dots, x_n)$.

Proof First of all, the extension

$$F(x_1, \ldots, x_n) \subset K$$

is Galois because K is the splitting field of $f(X)$ over $\mathbb{F}(x_1, \ldots, x_n)$. So the extension is normal. Also, $f(X) = \prod_{v \in V}(X - v)$ is separable. So we have

$$\mathbb{F}(x_1, \ldots, x_n) = K^G,$$

where $G =$ the Galois group of the extension. To prove Lemma B, we must show $G = \mathrm{GL}(V)$. Since the action of G on V determines the action on K, we have $G \subset \mathrm{GL}(V)$. Since the action of $\mathrm{GL}(V)$ on V, and hence on K, is faithful, we also have $\mathrm{GL}(V) \subset G$. ■

17 Poincaré series

In this section, we introduce the concept of the Poincaré series of a graded algebra and illustrate how it can be used to analyze the structure of rings of invariants. The main structural result is Molien's theorem, which is obtained in §17-2. The remaining sections are applications of that theorem. In particular, Molien's theorem is used in §17-3 to demonstrate how pseudo-reflections arise naturally in invariant theory. This is the first indication of an intrinsic relation between invariant theory and pseudo-reflections. Much of the remainder of this book will be concerned with the invariant theory of pseudo-reflection groups.

17-1 Poincaré series

A very useful way of gaining insight into the structure of rings of invariants is through their Poincaré series. A $\mathbb{F}$ vector space M is *graded* if there exists a decomposition $M = \bigoplus_{i\in\mathbb{Z}} M_i$, where each M_i is a subvector space. A graded $\mathbb{F}$ vector space $M = \bigoplus_{i\in\mathbb{Z}} M_i$ is *connected* if $M_i = 0$ for $i < 0$. It is of *finite type* if $\dim_{\mathbb{F}} M_i < \infty$ for all i. Notably, the symmetric algebra $S(V) = \bigoplus_{j=0}^{\infty} S_i(V)$ and the ring of invariants $S(V)^G = \bigoplus_{j=0}^{\infty} S_i^G(V)$ are graded, connected $\mathbb{F}$ vector spaces of finite type. Given a graded, connected $\mathbb{F}$ vector space M of finite type we can define its *Poincaré series*

$$P_t(M) = \sum_{i=0}^{\infty} (\dim_{\mathbb{F}} M_i) t^i.$$

Poincaré series satisfy both additive and multiplicative properties. Let M, M', M'' be graded connected $\mathbb{F}$ vector spaces of finite type. Then:

Multiplicative Property: $P_t(M \otimes_{\mathbb{F}} M') = P_t(M) P_t(M')$.

Additive Property: If $0 \to M' \to M \to M' \to 0$ is an exact sequence (i.e., $M' \subset M$ is a subvector space and $M'' = M/M'$, the quotient vector space) then

$$P_t(M) = P_t(M') + P_t(M').$$

In particular, this identity holds for direct sums $M = M' \oplus M'$.

Regarding the multiplicative property, $M \otimes_{\mathbb{F}} M'$ is defined by the rule

$$(M \otimes_{\mathbb{F}} M')_k = \sum_{i+j=k} M_i \otimes_{\mathbb{F}} M'_j.$$

So

$$\dim_{\mathbb{F}} (M \otimes_{\mathbb{F}} M')_k = \sum_{i+j=k} \dim_{\mathbb{F}}(M_i) \dim_{\mathbb{F}}(M').$$

Examples of Poincaré Series

Example 1: Let $M = \mathbb{F}[x]/(x^{n+1})$, where $\deg(x) = 1$. Then

$$P_t(M) = 1 + t + \cdots + t^n.$$

Example 2: Let $M = \mathbb{F}[x]/(x^{n+1})$, where $\deg(x) = d$. Then

$$P_t(M) = 1 + t^d + t^{2d} + \cdots + t^{nd}.$$

Example 3: Let $M = \mathbb{F}[x]$, where $\deg(x) = d$. Then

$$P_t(M) = 1 + t^d + t^{2d} + \cdots = \frac{1}{1 - t^d}.$$

Example 4: Let $M = \mathbb{F}[x_1, \ldots, x_n]$, where $\deg(x_i) = d_i$. We can write

$$M = \mathbb{F}[x_1] \otimes_{\mathbb{F}} \mathbb{F}[x_2] \otimes_{\mathbb{F}} \cdots \otimes_{\mathbb{F}} \mathbb{F}[x_n].$$

Example 3, with the multiplicative property of Poincaré series, then tells us that

$$P_t(M) = \left[\frac{1}{1 - t^{d_1}}\right]\left[\frac{1}{1 - t^{d_2}}\right]\cdots\left[\frac{1}{1 - t^{d_n}}\right].$$

Example 5: Let V be an n-dimensional $\mathbb{F}$ vector space and let $G \subset \mathrm{GL}(V)$ be a finite nonmodular subgroup. By Theorem 16-4B, we can write

$$S(V)^G = \bigoplus_{i=1}^{s} \mathbb{F}[x_1, \ldots, x_n]\alpha_i.$$

So

$$P_t\big(S(V)^G\big) = \frac{\sum_{i=1}^{s} t^{\deg(\alpha_i)}}{\prod_{i=1}^{n}(1 - t^{\deg(x_i)})}.$$

17-2 Molien's theorem

Molien's Theorem provides a very useful description of the Poincaré series of a ring of invariants. It states:

Theorem **(Molien)** *Let V be a finite dimensional $\mathbb{F}$ vector space. Let $G \subset \mathrm{GL}(V)$ be a finite nonmodular subgroup. Then*

$$P_t\big(S(V)^G\big) = \frac{1}{|G|}\sum_{\varphi \in G} \frac{1}{\det(1 - \varphi t)}.$$

Before proving the theorem, we shall give two concrete illustrations of its usefulness. These two examples will also make clear exactly how the notation in Molien's theorem is to be interpreted.

Example 1: Let $V = \mathbb{F}x \oplus \mathbb{F}y$, where $\operatorname{char}\mathbb{F} \neq 2$ and let $\mathbb{Z}/2\mathbb{Z} \subset \mathrm{GL}(V)$ be the subgroup generated by $\tau = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$. So τ interchanges x and y. Consider the following chart:

φ	$\det(1-\varphi t)$
$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$(1-t)^2$
$\tau = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$1-t^2$

By Molien's theorem,

$$P_t\big(S(V)^G\big) = \frac{1}{2}\left[\frac{1}{(1-t)^2} + \frac{1}{1-t^2}\right] = \frac{1}{(1-t)(1-t^2)}.$$

This suggests that $S(V)^G$ should be of the form $\mathbb{F}[f_1, f_2]$, where $\deg(f_1) = 1$ and $\deg(f_2) = 2$. This is exactly what happens. There are two obvious invariants:

$$f_1 = x + y \quad \text{and} \quad f_2 = xy.$$

Since the subalgebra $\mathbb{F}[f_1, f_2] \subset S(V)^G$ has the same Poincaré series as $S(V)^G$, it follows that $S(V)^G = \mathbb{F}[f_1, f_2]$.

***Example 2* (Stanley [1]):** Let $V = \mathbb{F}x \oplus \mathbb{F}y$, where $\operatorname{char}\mathbb{F} \neq 2$ and let $\mathbb{Z}/4\mathbb{Z} \subset \mathrm{GL}(V)$ be the subgroup generated by $\delta = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$. This time we have the chart:

φ	$\det(1-\varphi t)$
$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$(1-t)^2$
$\delta = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$	$1+t^2$
$\delta^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$	$(1+t)^2$
$\delta^3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$	$1+t^2$

By Molien's theorem,

$$P_t\big(S(V)^G\big) = \frac{1}{4}\left[\frac{1}{(1-t)^2} + \frac{2}{1+t^2} + \frac{1}{(1+t)^2}\right] = \frac{1+t^4}{(1-t^2)(1-t^4)}.$$

Keeping in mind the Cohen-Macauley property of $S(V)^G$, the above Poincaré series suggests that $S(V)^G$ should be of the form

$$S(V)^G = \mathbb{F}[f_1, f_2] + f_3\mathbb{F}[f_1, f_2],$$

where

$$\deg(f_1) = 2, \quad \deg(f_2) = 4 \quad \text{and} \quad \deg(f_3) = 4.$$

And this is exactly what happens. We have a subalgebra in $S(V)^G$ of the form $\mathbb{F}[f_1, f_2] + f_3\mathbb{F}[f_1, f_2]$ given by the polynomials

$$\begin{aligned} f_1 &= x^2 + y^2 \\ f_2 &= x^2y^2 \\ f_3 &= x^3y - xy^3. \end{aligned}$$

By comparing Poincaré series, we see that this subalgebra must be all of $S(V)^G$. Since we have the relation $f_3^2 = f_1^2 f_2 - 4f_2^2$, we can also rewrite $S(V)^G$ as

$$S(V)^G = \frac{\mathbb{F}[X, Y, Z]}{(Z^2 - X^2Y + 4Y^2)}.$$

As the above examples illustrate, Molien's theorem is very useful for calculating rings of invariants. We now set about proving the theorem. If V is a $\mathbb{F}$ vector space and $\varphi\colon V \to V$ is a linear map, we use

$$\varphi_i\colon S_i(V) \to S_i(V)$$

to denote the induced maps on the graded components of $S(V)$. Molien's theorem is based on the following trace formula.

Proposition A *Given a finite dimensional* $\mathbb{F}$ *vector space* V *and a linear map* φ: $V \to V$, *then*

$$\sum_{i=0}^{\infty} \operatorname{tr}(\varphi_i)t^i = \frac{1}{\det(1 - \varphi t)}.$$

Proof We shall work in the algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$. Then V has a basis $\{t_1, \ldots, t_n\}$ with respect to which the matrix of φ is upper triangular, i.e.,

$$\varphi = \begin{bmatrix} \lambda_1 & * & \cdots & * \\ 0 & \lambda_2 & & \vdots \\ \vdots & & \ddots & * \\ 0 & \cdots & 0 & \lambda_n \end{bmatrix}$$

We can write $S(V) = \overline{\mathbb{F}}[t_1, \ldots, t_n]$. So $S_i(V)$ has a basis $\{t_1^{j_1} \cdots t_n^{j_n} \mid j_1 + \cdots + j_n = i\}$. If we order this basis correctly (lexicographically! See Remark, below), then φ_i is represented by an upper triangular matrix with $\{\lambda_1^{j_1} \cdots \lambda_n^{j_n} \mid j_1 + \cdots + j_n = i\}$ down the diagonal. So

$$\operatorname{tr}(\varphi_i) = \sum_{j_1 + \cdots + j_n = i} \lambda_1^{j_1} \cdots \lambda_n^{j_n}.$$

It follows that

$$\begin{aligned}\sum_{i=0}^{\infty}\mathrm{tr}(\varphi_i)t^i &= \sum_{i=0}^{\infty}\Big[\sum_{j_1+\cdots+j_n=i}\lambda_1^{j_1}\cdots\lambda_n^{j_n}\Big]t^i\\ &= \Big[\sum_{j_1}\lambda_1^{j_1}t^{j_1}\Big]\cdots\Big[\sum_{j_n}\lambda_n^{j_n}t^{j_n}\Big]\\ &= \frac{1}{1-\lambda_1 t}\cdots\frac{1}{1-\lambda_n t}=\frac{1}{\det(1-\varphi t)}.\end{aligned}$$ ∎

Remark: The *lexicographic ordering* mentioned in the above proof is defined as follows: given two monomials $t_1^{i_1}\cdots t_n^{i_n}$ and $t_1^{j_1}\cdots t_n^{j_n}$ in $S_i(V)$, we say that

$$t_1^{i_1}\cdots t_n^{i_n} < t_1^{j_1}\cdots t_n^{j_n},$$

if there exists k such that $i_s = j_s$ for $s > k$, but $i_k < j_k$. For example, $t_1 < t_2 < \cdots < t_n$.

Our second proposition is the means by which the above trace formula is translated into Molien's theorem. We use representation theory, as outlined in Appendix B, to relate invariants and traces.

Proposition B *Given a finite dimensional* $\mathbb{F}$ *vector space* W*, and a finite nonmodular subgroup* $G \subset \mathrm{GL}(W)$*, then*

$$\dim_{\mathbb{F}} W^G = \frac{1}{|G|}\sum_{\varphi\in G}\mathrm{tr}(\varphi).$$

Proof The hypothesis ensures that Maschke's theorem from Appendix B applies. So if we regard W as a G module, then we can decompose W as a direct sum of irreducible G modules. In particular, the irreducible trivial representation ($\varphi\cdot x = x$ for all $x \in W$) is one-dimensional and W^G is the sum of copies of this irreducible representation. If we let

$$\chi = \text{the character of } \rho\colon G \longrightarrow \mathrm{GL}(W)$$

$$\mathcal{E} = \text{the character of the irreducible trivial representation}$$

$$\text{i.e., } \mathcal{E}(\varphi) = 1 \quad \text{for all } \varphi \in G,$$

then the standard inner product for characters

$$(\chi, \mathcal{E}) = \frac{1}{|G|}\sum_{\varphi\in G}\chi(\varphi)\mathcal{E}(\varphi)$$

counts the number of copies of the irreducible trivial representation in ρ. So we have

$$\dim_{\mathbb{F}} W^G = (\chi,\mathcal{E}) = \frac{1}{|G|}\sum_{\varphi\in G}\chi(\varphi)\mathcal{E}(\varphi) = \frac{1}{|G|}\sum_{\varphi\in G}\chi(\varphi).$$ ∎

Proof of Molien's Theorem For each $\varphi\colon V \to V$, we have the induced maps

$$\varphi_i\colon S_i(V) \to S_i(V).$$

By Proposition B, we have the identity

$$(*) \qquad \dim S_i^G(V) = \frac{1}{|G|}\sum_{\varphi\in G} \operatorname{tr}(\varphi_i).$$

Consequently,

$$\begin{aligned} P_t\big(S(V)^G\big) &= \sum_{i=0}^{\infty}[\dim S_i^G(V)]t^i = \sum_{i=0}^{\infty}\frac{1}{|G|}\sum_{\varphi\in G}\operatorname{tr}(\varphi_i) \quad \text{by } (*)\\ &= \frac{1}{|G|}\sum_{\varphi\in G}\Big[\sum_{i=0}^{\infty}\operatorname{tr}(\varphi_i)t^i\Big] = \frac{1}{|G|}\sum_{\varphi\in G}\frac{1}{\det(1-\varphi t)} \quad \text{by Proposition A.}\end{aligned}$$

Poincaré Series of $S(V^*)^G$ If we consider the invariants $S(V^*)^G$ obtained from $G \subset \mathrm{GL}(V)$, then we obtain the slightly different identity

$$P_t\big(S(V^*)^G\big) = \frac{1}{|G|}\sum_{\varphi\in G}\frac{1}{\det(1-\varphi^{-1}t)}.$$

This difference can be traced to the identity

$$\langle \varphi\cdot x, y\rangle = \langle x, \varphi^{-1}\cdot y\rangle$$

from §16-1.

Since we are summing over all elements of G, the right-hand side of the Molien identity for $P_t\big(S(V)^G\big)$ and $P_t\big(S(V^*)^G\big)$ is the same, i.e., *both* $R = S(V)^G$ *and* $R^* = S(V^*)^G$ *have the same Poincaré series in the nonmodular case.* See §18-1 for an application of this fact.

17-3 Molien's theorem and pseudo-reflections

We can use Molien's theorem to provide a link between invariant theory and pseudo-reflections. We finish this section by proving that information about the pseudo-reflections of $G \subset \mathrm{GL}(V)$ is present in the Poincaré series of the ring of invariants $S(V)^G$. The implications of this relation will be demonstrated in the next section.

We shall only consider the nonmodular case. So assume that V *is a finite dimensional* $\mathbb{F}$ *vector space, and that* $G \subset \mathrm{GL}(V)$ *is a finite nonmodular subgroup.* We

can use Molien's theorem to obtain an expansion of $P_t\left(S(V)^G\right)$ as a Laurent series in the variable $(1-t)$.

Lemma $P_t\left(S(V)^G\right) = \frac{1}{|G|}\left[\frac{1}{(1-t)^n} + \frac{C_{n-1}}{(1-t)^{n-1}} + \cdots\right]$, *where* $n = \dim_{\mathbb{F}} V$ *and*

$$2C_{n-1} = \textit{the number of pseudo-reflections in } G.$$

The rest of the section is devoted to the proof of this lemma. We have, by Molien's theorem, the equality

$$P_t\left(S(V)^G\right) = \frac{1}{|G|}\sum_{\varphi\in G}\frac{1}{\det(1-\varphi t)}.$$

We prove the lemma by expanding the right-hand side of this equality as a Laurent series in the variable $(1-t)$ and explicitly determining the first few coefficients. We have, for each $\varphi \in G$, a decomposition

$$\det(1-\varphi t) = f(t)(1-t)^k$$

into relatively prime factors, where

$$k = \dim_{\mathbb{F}} V^{\varphi}.$$

It follows that we can write

$$\frac{1}{|G|}\sum_{\varphi\in G}\frac{1}{\det(1-\varphi t)} = \frac{1}{(1-t)^n} + \sum_s \frac{1}{(1-t)^{n-1}(1-\xi_s t)} + \cdots,$$

where s ranges through the pseudo-reflections of G and ξ_s is the nontrivial eigenvalue of s. Consequently, we have a Laurent series expansion

$$\frac{1}{|G|}\sum_{\varphi\in G}\frac{1}{\det(1-\varphi t)} = \frac{1}{(1-t)^n} + \frac{C_{n-1}}{(1-t)^{n-1}} + \cdots,$$

where C_{n-1} also appears in the expansion

$$\sum_s \frac{1}{(1-t)^{n-1}(1-\xi_s t)} = \frac{C_{n-1}}{(1-t)^{n-1}} + \frac{C_{n-2}}{(1-t)^{n-2}} + \cdots.$$

To determine C_{n-1}, multiply by $(1-t)^{n-1}$ and let $t=1$. We obtain

$$\sum_s \frac{1}{1-\xi_s} = C_{n-1}.$$

Now, s is a pseudo-reflection if and only if s^{-1} is a pseudo-reflection. Thus we can rewrite the above as

$$\sum_s \frac{1}{1-\xi_s^{-1}} = C_{n-1}.$$

Adding the last two equations and using the identity

$$\frac{1}{1-\xi_s} + \frac{1}{1-\xi_s^{-1}} = 1,$$

we obtain $2C_{n-1} =$ the number of pseudo-reflections in G.

17-4 Polynomial algebras as rings of invariants

We now use the machinery of Poincaré series to deduce important relations between the structure of the group $G \subset \mathrm{GL}(V)$ and the structure of its ring of invariants $S(V)^G$. We are mainly concerned with the case of $S(V)^G$ being a polynomial algebra. In each argument that follows, the technique will be to compare two different expressions for the Poincaré series of $S(V)^G$. The expressions will be Laurent series expansions in the variable $(1-t)$, with one of the expressions being given by the lemma from §17-3. We shall compare the coefficients of $1/(1-t)^n$ and of $1/(1-t)^{n-1}$ from the two different expressions.

Theorem A *Let V be a finite dimensional $\mathbb{F}$ vector space. Let $G \subset \mathrm{GL}(V)$ be a finite nonmodular subgroup. Suppose*

$$S(V)^G = \mathbb{F}[x_1, \ldots, x_n] \quad \textit{where } d_i = \deg x_i.$$

Then

(i) $|G| = d_1 \cdots d_n$;
(ii) the number of pseudo-reflections in G is $(d_1 - 1) + \cdots + (d_n - 1)$.

Proof (i) As in Example 4 from §17-1, we can write

$$P_t\big(S(V)^G\big) = \frac{1}{\prod_{i=1}^n (1 - t^{d_i})} = \frac{1}{(1-t)^n \prod_{i=1}^n (1 + t + \cdots + t^{d_i - 1})}.$$

On the other hand, by Lemma 17-3, we can write

$$P_t\big(S(V)^G\big) = \frac{1}{|G|}\left[\frac{1}{(1-t)^n} + \frac{C_{n-1}}{(1-t)^{n-1}} + \cdots\right],$$

where $2C_{n-1}$ = the number of pseudo-reflections in G. If we equate the two expressions for $P_t\big(S(V)^G\big)$ and multiplies by $(1-t)^n$, then we obtain

$$(*) \qquad \frac{1}{\prod_{i=1}^n (1 + t + \cdots + t^{d_i - 1})} = \frac{1}{|G|}[1 + C_{n-1}(1-t) + \cdots].$$

This can be rewritten as

$$|G| = \left[\prod_{i=1}^n (1 + t + \cdots + t^{d_i - 1})\right][1 + C_{n-1}(1-t) + \cdots].$$

Letting $t = 1$, we have $|G| = \prod_{i=1}^n d_i$.

(ii) If we take equation $(*)$ from above and differentiate with respect to t (using logarithmic differentiation), then we obtain

$$\frac{1}{\prod_{i=1}^n (1 + t + \cdots + t^{d_i - 1})}\left[-\sum_{i=1}^n \frac{1 + 2t + \cdots + (d_i - 1)t^{d_i - 2}}{1 + t + \cdots + t^{d_i - 1}}\right]$$
$$= \frac{1}{|G|}[-C_{n-1} - 2C_{n-2}(1-t) - \cdots].$$

Letting $t = 1$, we have

$$\frac{1}{|G|}C_{n-1} = \frac{1}{(\prod_{i=1}^{n} d_i)}\left[\sum_{i=1}^{n} \frac{d_i(d_i-1)}{2d_i}\right].$$

Hence,

$$2C_{n-1} = \sum_{i=1}^{n}(d_i - 1).$$

■

See §31-1 for a significant generalization, due to Solomon, of Theorem A.

We next produce a technical, but useful, extension of Theorem A. Given a finite group $G \subset \mathrm{GL}(V)$, we know from the Noether normalization theorem (see §16-4) that there exists a polynomial subalgebra $\mathbb{F}[x_1,\ldots,x_n] \subset S(V)^G$ such that $S(V)^G$ is finite over $\mathbb{F}[x_1,\ldots,x_n]$.

Theorem B *Let V be a finite dimensional $\mathbb{F}$ vector space. Let $G \subset \mathrm{GL}(V)$ be a finite nonmodular subgroup. Given $\mathbb{F}[x_1,\ldots,x_n] \subset S(V)^G$, suppose $S(V)^G$ is finite over $\mathbb{F}[x_1,\ldots,x_n]$. Let $d_i = \deg x_i$. Then*

(i) $|G|$ divides $d_1 \cdots d_n$
(ii) $S(V)^G = \mathbb{F}[x_1,\ldots,x_n]$ if and only if $|G| = d_1 \cdots d_n$.

Proof Lemma 16-4 demonstrates that $S(V)^G$ is free over $\mathbb{F}[x_1,\ldots,x_n]$. Write

$$S(V)^G = \bigoplus_{i=1}^{s} \mathbb{F}[x_1,\ldots,x_n]\alpha_i.$$

So

$$P_t\big(S(V)^G\big) = \frac{t^{\deg(\alpha_i)} + \cdots + t^{\deg(\alpha_s)}}{\prod_{i=1}^{n}(1-t^{d_i})}.$$

By mimicking the proof of Theorem A, we obtain

$$s|G| = d_1 \cdots d_n.$$

Then (i) and (ii) follow. ■

17-5 The algebra of covariants

The *algebra of covariants* is the quotient algebra $S(V)/I$, where

$$I = \text{the ideal of } S(V) \text{ generated by } S(V)^G_+ = \sum_{k\geq 1} S_k(V)^G.$$

In other words, I is generated by the homogeneous elements from $S(V)^G$ of positive degree.

In this section, we shall study the relation between the structure of $S(V)/I$ and the structure of $S(V)$ as a module over $S(V)^G$. This relation will play an important role in future chapters, appearing prominently in Chapter 18. It will be further analyzed in Chapters 25 and 26. This section will be devoted to proving:

Theorem *Let V be a finite dimensional $\mathbb{F}$ vector space. Let $G \subset \mathrm{GL}(V)$ be a finite nonmodular subgroup. Then* $\dim_{\mathbb{F}} S(V)/I \geq |G|$ *with equality if and only if $S(V)$ is a free $S(V)^G$ module.*

This theorem will be used in §26-5. We begin the proof of the theorem with a standard algebraic fact.

Lemma *If $\{\bar{e}_q\}$ is a homogeneous $\mathbb{F}$ basis of $S(V)/I$, and $\{e_q\}$ are homogeneous representatives in $S(V)$, then $\{e_q\}$ generate $S(V)$ as a $S(V)^G$ module, i.e.,*

$$S(V) = \sum_q S(V)^G e_q.$$

Proof By induction on degree. Given $f \in S_k(V)$, we can expand

$$f = \sum_q \lambda_q e_q + d, \quad \text{where } \lambda_q \in \mathbb{F} \text{ and } d \in I_k.$$

By the definition of I, we can also expand

$$d = \sum_{i+j=k} c_i d_j, \quad \text{where } c_i \in S_i(V) \text{ and } d_j \in S_j(V)^G.$$

Deg $d_j > 0$ implies $\deg c_i < k$. By induction, each c_i belongs to the $S(V)^G$ module generated by $\{e_q\}$. Hence, d and f belong as well. ■

The Poincaré series results of the previous section will play a key role in our arguments. In proving the theorem, it will be convenient to adopt the following inequality relation for elements in the power series ring $\mathbb{Z}[[t]]$.

Definition: Given $f(t), g(t) \in \mathbb{Z}[[t]]$ with expansions

$$f(t) = \sum_{i\geq 0} f_i t^i \quad \text{and} \quad g(t) = \sum_{i\geq 0} g_i t^i,$$

then $f(t) \leq g(t)$ if $f_i \leq g_i$ for all i.

Remark: If $f(t)$ and $g(t)$ are polynomials, then $f(1)$ and $g(1)$ are well defined. Moreover, if $f(t)$ and $g(t)$ are polynomials with positive integer coefficients and $f(t) \leq g(t)$, then

$$f(1) \leq g(1)$$
$$f(t) = g(t) \quad \text{if and only if} \quad f(1) = g(1).$$

Proof of Theorem Let $P(t)$ = the Poincaré polynomial of $S(V)/I$ and, as in Example 5 from §16-1, let

$$\frac{f(t)}{\prod_{i=1}^{n}(1-t^{d_i})} = \text{the Poincaré polynomial of } S(V)^G.$$

By the above lemma, any homogeneous set Γ of representatives in $S(V)$ of an $\mathbb{F}$ basis of $S(V)/I$ generates $S(V)$ as a $S(V)^G$ module. In other words,

$$S(V) = S(V)^G\Gamma$$

and, so, we have the inequality of power series

$$(*) \qquad 1/(1-t)^n \leq \left[f(t)/\prod(1-t^{d_i})\right]P(t)$$

with equality if and only if $S(V)$ is a free $S(V)^G$ module. We can simplify to obtain the inequality of polynomials

$$(**) \qquad \prod(1+t+\cdots+t^{d_i-1}) \leq f(t)P(t).$$

And, again, we have equality if and only if $S(V)$ is a free $S(V)^G$ module. Next, we substitute $t = 1$ into this inequality and obtain

$$(***) \qquad \prod d_i \leq f(1)P(1).$$

By the remarks preceding the proof, we have equality for $(**)$ if and only if we have equality for $(***)$. Thus $\prod d_i = f(1)P(1)$ if and only if $S(V)$ is a free $S(V)^G$ module.

We can make further alterations in $(***)$. We have the identity

$$P(1) = \dim_{\mathbb{F}} S(V)/I.$$

Also, if we let

$$s = f(1),$$

then, by the argument used to prove Theorem B of §17-4, we have $\prod d_i = s|G|$.

By substituting these identities into $(***)$, we obtain the inequality

$$s|G| \leq s\big(\dim_{\mathbb{F}} S(V)/I\big)$$

with equality if and only if $S(V)$ is a free $S(V)^G$ module. Lastly, cancel s. ∎

18 Nonmodular invariants of pseudo-reflection groups

This chapter proves a remarkable correspondence arising from the work of Chevalley [1]. It will be shown that, in the nonmodular case, the ring of invariants of a finite pseudo-reflection group is a polynomial algebra and, furthermore, that this property actually characterizes nonmodular finite pseudo-reflection groups.

18-1 The main result

The concept of a graded polynomial algebra $\mathbb{F}[x_1, \dots, x_n]$ was introduced in §1-7. Most of this chapter is devoted to proving

Theorem **(Chevalley-Shephard-Todd-Bourbaki)** *Let V be a finite dimensional vector space over a field $\mathbb{F}$. Given a finite nonmodular subgroup $G \subset \mathrm{GL}(V)$, then G is a pseudo-reflection group if and only if $S(V)^G$ is a polynomial algebra.*

In view of the discussion from §17-4, if $G \subset \mathrm{GL}(V)$ is a finite pseudo-reflection group, where $\operatorname{char} \mathbb{F}$ does not divide $|G|$, and if we write

$$S(V)^G = \mathbb{F}[x_1, \dots, x_n] \quad \text{where } d_i = \deg x_i,$$

then:

Corollary A

(i) $|G| = \prod_{i=1}^n d_i$*;*
(ii) the number of reflections in G is $\sum_{i=1}^n (d_i - 1)$.

The integers $\{d_1, \dots, d_n\}$ are called the *degrees* of G, whereas the integers $\{m_1, \dots, m_n\}$, where $m_i = d_i - 1$, are called the *exponents* of G. The choice of the algebra generators $\{x_1, \dots, x_n\}$ is far from unique. On the other hand, an argument using Poincaré series easily establishes that the degrees $\{d_1, \dots, d_n\}$, and, hence, the exponents $\{m_1, \dots, m_n\}$, are unique (see, for example, the discussion at the end of §17-2). Much of the discussion in subsequent chapters will be focused on ways of calculating the degrees/exponents of pseudo-reflection groups. In particular, in the last section of this chapter, we show that we already have enough information to make significant statements about the degrees of Euclidean reflection groups.

Remark 1: The theorem above only partly extends to the modular case. $S(V)^G$ polynomial forces G to be a pseudo-reflection group but, conversely, the invariants of a pseudo-reflection group need not form a polynomial algebra. This will be discussed in Chapter 19.

Remark 2: If we dualize and consider the action of G on V^*, then $G \subset \mathrm{GL}(V^*)$ is also a pseudo-reflection group and, so, the ring of invariants $S(V^*)^G$ is a polynomial algebra as well. There is a close relation between the two polynomial algebras $S(V)^G$ and $S(V^*)^G$. Write

$$R = \mathbb{F}[x_1, \dots, x_n] \quad \text{and} \quad R^* = \mathbb{F}[\alpha_1, \dots, \alpha_k].$$

Let

$$d_i = \deg x_i \quad \text{and} \quad d_i^* = \deg \alpha_i.$$

We want to point out a fact that will be used in §32-3, namely *the degrees* $\{d_1, \dots, d_n\}$ *of* $S(V)^G$ *and* $\{d_1^*, \dots, d_k^*\}$ *of* $S(V^*)^G$ *are the same.* In other words, $k = n$ and, further, we can arrange the generators so that $d_i = d_i^*$. We now justify this fact modulo one result that will not be established until §23-2. It was observed at the end of §17-2 that $S(V)^G$ and $S(V^*)^G$ have the same Poincaré series. Moreover, by Example 4 in §17-1, the Poincaré series of $S(V)^G$ and $S(V^*)^G$ can be written

$$P_t\big(S(V)^G\big) = \frac{1}{(1-t^{d_1})(1-t^{d_2})\cdots(1-t^{d_n})}$$

$$P_t\big(S(V^*)^G\big) = \frac{1}{(1-t^{d_1^*})(1-t^{d_2^*})\cdots(1-t^{d_k^*})}.$$

Thus $(1-t^{d_1})(1-t^{d_2})\cdots(1-t^{d_n}) = (1-t^{d_1^*})(1-t^{d_2^*})\cdots(1-t^{d_k^*})$. But Lemma 23-2 shows that a decomposition of the form $f(t) = (1-t)^{e_1}(1-t^2)^{e_2}\cdots(1-t^k)^{e_k}$ is unique. Thus the sets $\{d_1, \dots, d_n\}$ and $\{d_1^*, \dots, d_k^*\}$ must agree.

The rest of this chapter is devoted to the proof of the main theorem. We shall prove the equivalence of the following conditions:

(i) $G \subset GL(V)$ is a pseudo-reflection group
(ii) $S(V)$ is a free $S(V)^G$ module
(iii) $S(V)^G$ is a polynomial algebra.

After developing some machinery in §18-2, we shall prove in §18-3 that $S(V)$ is a free $S(V)^G$ module when $G \subset GL(V)$ is a nonmodular pseudo-reflection group. In §18-4, we shall show that $S(V)$ being a free $S(V)^G$ module forces $S(V)^G$ to be polynomial. In §18-5, we shall prove that $S(V)^G$ polynomial forces $G \subset GL(V)$ to be a pseudo-reflection group.

Throughout this chapter, we shall make the assumption that V *is a finite dimensional vector space over the field* $\mathbb{F}$, *and* $G \subset GL(V)$ *is a finite nonmodular subgroup.*

Notation: In order to simplify notation, we also let

$$S = S(V) \text{ and } R = S(V)^G$$

$$I = I_G = \text{the graded ideal of } S \text{ generated by } R_+ = \sum_{i \geq 1} R_i.$$

18-2 The Δ operators

For each pseudo-reflection $s\colon V \to V$, we can define an operation

$$\Delta\colon S \to S$$

that lowers degree by 1. Recall, from §14-3, that s has a decomposition

$$(*) \qquad s \cdot x = x + \Delta(x)\alpha$$

for all $x \in V$. Here α generates $\mathrm{Im}(s-1)$ and

$$\Delta \colon V \to \mathbb{F}$$

is a linear form. The operation $\Delta \colon S \to S$ will be an extension of this linear form.

We define $\Delta \colon S \to S$ by demanding that $(*)$ hold for an arbitrary $x \in S$. We can use the multiplicative identity $s \cdot (xy) = (s \cdot x)(s \cdot y)$ to extend the decomposition $(*)$ from $s \cdot x$ and $s \cdot y$ to $s \cdot (xy)$. Namely, if

$$s \cdot x_1 = x_1 + \lambda_1 \alpha \quad \text{and} \quad s \cdot x_2 = x_2 + \lambda_2 \alpha,$$

then

$$\begin{aligned} s \cdot (x_1 x_2) = (s \cdot x_1)(s \cdot x_2) &= (x_1 + \lambda_1 \alpha)(x_2 + \lambda_2 \alpha) \\ &= x_1 x_2 + (x_1 \lambda_2 + \lambda_1 x_2 + \lambda_1 \lambda_2 \alpha)\alpha. \end{aligned}$$

Since S is generated, as an algebra, by $S_1 = V$, such a decomposition of $s \cdot x$ is thereby forced for every $x \in S$.

The operations Δ are *twisted derivations*, namely they satisfy:

Lemma A *For any $x, y \in S$, $\Delta(xy) = \Delta(x)y + (s \cdot x)\Delta(y)$.*

Proof From $(*)$, we have the identities

$$\begin{aligned} s \cdot x &= x + \Delta(x)\alpha \\ s \cdot y &= y + \Delta(y)\alpha \\ s \cdot (xy) &= xy + \Delta(xy)\alpha. \end{aligned}$$

The multiplicative identity $s \cdot (xy) = (s \cdot x)(s \cdot y)$ then gives us

$$\Delta(xy) = \Delta(x)y + x\Delta(y) + \Delta(x)\Delta(y)\alpha.$$

Combining this with the first identity, we have the lemma. ■

Now assume that $s \in G$. If we consider S as an R module through the inclusion $S \subset R$, then we also have:

Lemma B *$\Delta \colon S \to S$ is a map of R modules, i.e., for any $x \in R$ and $y \in S$ we have*

$$\Delta(xy) = x\Delta(y).$$

Proof This follows from Lemma A, and the fact that $\Delta(x) = 0$ and $s \cdot x = x$, since $x \in R$. ∎

It follows from Lemma B that the Δ operation associated to each $s \in G$ induces a well-defined map on the quotient algebra S/I. The action of Δ on S/I is highly nontrivial. The following fact will play an important role in §18-3.

Lemma C *Assume that $G \subset \mathrm{GL}(V)$ is a pseudo-reflection group. If $0 \neq x \in S/I$ is a homogeneous element of degree > 0, then there exists a pseudo-reflection $s \in G$ such that its associated twisted derivation Δ satisfies $\Delta(x) \neq 0$.*

Proof We shall show that $\Delta(x) = 0$ for all twisted derivations Δ forces $x = 0$. First of all, $\Delta(x) = 0$ for all twisted derivations Δ is equivalent to asserting that $s \cdot x = x$ for all pseudo-reflections $s \in G$. Since G is generated by pseudo-reflections, we have

$$\varphi \cdot x = x \quad \text{for all } \varphi \in G.$$

Averaging (here we are using the assumption from §18-1 that char $\mathbb{F}$ does not divide $|G|$), we obtain

$$\mathrm{Av}(x) = \frac{1}{|G|} \sum_{\varphi \in G} \varphi \cdot x = x.$$

Since $\mathrm{Im}\,\mathrm{Av} = R$ in S, it follows that $\mathrm{Av} = 0$ in S/I. So $x = 0$ in S/I. ∎

18-3 S as a free R module

We know from the proof of the Cohen-Macauley theorem in §16-4 that S is a finitely generated R module. In other words, S/I is a finite dimensional $\mathbb{F}$ vector space. This result only depends on G being a finite group. We now prove:

Proposition *If $G \subset \mathrm{GL}(V)$ is a finite pseudo-reflection group, then S is a free R module.*

To prove the proposition, regard S/I as a graded $\mathbb{F}$ vector space. Pick a basis $\{\bar{e}_q\}$ of S/I and let $\{e_q\}$ be representatives in S for these elements. It was shown in Lemma 17-5 that S is generated, as an R module, by $\{e_q\}$. The following lemma shows that, in the pseudo-reflection case, S is actually freely generated as an R module by $\{e_q\}$. In all that follows, we shall deal with homogeneous elements in S and S/I.

Lemma *If $\{\bar{e}_q\}$ is a homogeneous basis of S/I, and $\{e_q\}$ are homogeneous representatives in S, then the elements $\{e_q\}$ are independent over R.*

Proof First of all, given any relation

$$(*) \qquad x_1 e_{q_1} + \cdots + x_\ell e_{q_\ell} = 0,$$

where $0 \neq x_i \in R$, then

$(**)$ the elements $\{x_i\}$ are linearly dependent over $\mathbb{F}$.

For, assume that $\deg e_{q_1} = d$ is maximal among $\{\deg e_{q_i}\}$. By Lemma 18-2C, we can find twisted derivations $\{\Delta_1, \dots, \Delta_d\}$ such that

$$\Delta = \Delta_1 \cdots \Delta_d$$

satisfies $0 \neq \Delta(e_{q_1}) \in S_0 = \mathbb{F}$. If we apply Δ to relation $(*)$, then, by Lemma 18-2B, we obtain

$$0 = \Delta(x_1 e_{q_1} + \cdots + x_\ell e_{q_\ell}) = x_1 \Delta(e_{q_1}) + \cdots + x_\ell \Delta(e_{q_\ell}).$$

Moreover ,

$$\begin{aligned} \Delta(e_{q_i}) &= 0 \quad \text{if } \deg e_{q_i} < d \\ \Delta(e_{q_i}) &\in \mathbb{F} \quad \text{if } \deg e_{q_i} = d. \end{aligned}$$

Since $\Delta(e_{q_1}) \neq 0$, we have a nontrivial $\mathbb{F}$ linear combination among the $\{x_i\}$.

Now, suppose that a relation of the form $(*)$ exists. Pick such a relation involving a minimal number of elements for any choice of $\{\bar{e}_q\}$ and $\{e_q\}$. Then $(**)$ implies that we can write

$$x_1 = \lambda_2 x_2 + \cdots + \lambda_\ell x_\ell,$$

where $\lambda_i \in \mathbb{F}$ and $\ell \geq 2$. And relation $(*)$ can be rewritten

$$x_2 \bar{e}_2 + \cdots + x_\ell \bar{e}_\ell = 0,$$

where

$$\bar{e}_i = e_{q_i} + \lambda_i e_{q_1}.$$

So we have contradicted the minimality of our choice of relation. Thus no relation of the form $(*)$ can exist. ■

18-4 R as a polynomial algebra

In this section, we prove:

Proposition *If S is a finitely generated free R module, then R is a polynomial algebra $\mathbb{F}[f_1, \dots, f_\ell]$.*

First of all, we must choose the generators $\{f_1, \dots, f_\ell\}$. By §16-5, R is finitely generated as an algebra. Let $\{f_1, \dots, f_\ell\}$ be a minimal generating set of R. Next, we want to show that $\{f_1, \dots, f_\ell\}$ are algebraically independent. We do this by showing that any algebraic relation between $\{f_1, \dots, f_\ell\}$ forces a linear relation over R between the elements $\{f_1, \dots, f_\ell\}$. Namely, for some i, we can write f_i as an R linear combination of $\{f_j\}_{j \neq i}$. This contradicts the minimality of $\{f_1, \dots, f_\ell\}$. So no such algebraic relation can exist.

We shall do the proof twice. First of all, we do the proof with a simplifying hypothesis. Then we make the necessary alterations so that the proof works without the hypothesis. In all that follows, we assume that P is a nonzero polynomial giving an algebraic relation between $\{f_1, \ldots, f_\ell\}$, i.e.,

$$P(f_1, \ldots, f_\ell) = 0.$$

We write

$$S = \mathbb{F}[t_1, \ldots, t_n],$$

and let

$$P_i = \frac{\partial P}{\partial f_i} \quad (1 < i < \ell) \quad \text{and} \quad f_{ij} = \frac{\partial f_i}{\partial t_j} \quad (1 \leq i \leq \ell, 1 \leq j \leq n)$$

denote the formal derivatives of the polynomials $P = P(f_1, \ldots, f_\ell)$ and $f_i = f_i(t_1, \ldots, t_n)$.

Part I: Simplified Proof We first produce an R linear relation between the generators $\{f_1, \ldots, f_\ell\}$ under the assumption that *no proper subset of* $\{P_1, \ldots, P_\ell\}$ *generates the ideal* $(P_1, \ldots, P_\ell) \subset S$. There is no reason to assume that this minimality assumption is always true. In Part II, we shall drop this assumption and give the general proof. So the strategy of our proof is heuristic. We want to begin with a simpler and, hopefully, clearer proof before giving the general proof.

If we can show that, for all i, j:

Lemma A *$f_{ij} \in$ the ideal $(f_1, \ldots, f_\ell) \subset S$.*

Then we can force the desired type of R linear relations among the elements $\{f_1, \ldots, f_\ell\}$ because we have the Euler identity

$$(*) \qquad d_i f_i = \sum_j f_{ij} t_j, \quad \text{where } d_i = \deg f_i.$$

Moreover, we can always choose i such that

$$(**) \qquad d_i \neq 0$$

in $\mathbb{F}$. This only needs comment for char $\mathbb{F} = p > 0$. In order to show that one of the algebra generators of $R = S^G$ has degree $\neq 0 \pmod p$, it suffices to show that R has a nontrivial element of degree $\neq 0 \pmod p$. We are assuming that $|G| \neq 0 \pmod p$. The desired result then follows from the fact that, for all $x \in V$, $\prod_{\varphi \in G}(\varphi \cdot x)$ has degree $|G|$ and is invariant under G.

It follows from $(*)$ and $(**)$ that we can expand f_i as an S linear combination

$$(***) \qquad f_i = \sum_{j \neq i} \lambda_j f_j, \quad \text{where } \lambda_j \in S$$

of the elements $\{f_j\}_{j\neq i}$. (Expand each f_{ij} as an S linear combination of $\{f_1, \ldots, f_\ell\}$, substitute into the RHS of $(*)$ and take the component of degree d_i.)

Lastly, the terms λ_i in $(***)$ actually belong to R. For, by the Cohen-Macauley property of §16-4, S is a free R module, i.e.,

$$S = \bigoplus_k \mathrm{R}e_k\,.$$

And it can always be arranged that one of the summands is the canonical inclusion $R \subset S$, i.e., $e_k = 1$ for some k. Now consider $(***)$. We have $f_i \in R \subset S$. So if we expand the coefficients $\{\lambda_j\}$ in the RHS of $(***)$ with respect to the decomposition $S = \bigoplus_k \mathrm{R}e_k$, and take the components lying in the summand $R \subset S$, we have the desired relation

$$f_i = \sum_{j\neq i} \bar{\lambda}_j f_j, \quad \text{where } \bar{\lambda}_j \in R.$$

Thus we are left with proving Lemma A.

Proof of Lemma A Since $f_{ij} \in S = \bigoplus_k \mathrm{R}e_k$, we can expand

(i) $f_{ij} = \sum_k \rho_{ijk}e_k$, where $\rho_{ijk} \in R$: To prove the lemma, it suffices to show

$$\deg \rho_{ijk} > 0$$

for each k. Because the $\{f_1\}$ generate a polynomial subalgebra of S, if we differentiate $P(f_1, \ldots, f_\ell) = 0$ with respect to t_j, then the chain rule gives

(ii) $\sum_i P_i f_{ij} = 0$: Substituting (i) into (ii), we have

$$0 = \sum_i P_i\Big[\sum_k \rho_{ijk}e_k\Big] = \sum_k \Big[\sum_i P_i\rho_{ijk}\Big]e_k.$$

Since S is freely generated over R by $\{e_k\}$, we have

(iii) $\sum_i P_i\rho_{ijk} = 0$ for each k: These identities force $\deg \rho_{ijk} > 0$ whenever $\rho_{ijk} \neq 0$. Otherwise, ρ_{ijk} would be a constant and P_i would be an S linear combination of $\{P_j\}_{j\neq i}$. This contradicts our assumption that $\{P_1, \ldots, P_\ell\}$ is a minimal generating set of $(P_1, \ldots, P_\ell)$. ■

Part II: General Proof We now turn to the general proof. Although the previous assumption no longer holds, we can always order $\{P_1, \ldots, P_\ell\}$ in such a way that there exists $m < \ell$ so that, *among the subsets of* $\{P_1, \ldots, P_\ell\}$, *the set* $\{P_1, \ldots, P_m\}$ *is a minimal generating set of the ideal* $(P_1, \ldots, P_\ell) \subset S$.

Then for $j > m$, we can write

$$P_j = \sum_{i=1}^{m} \delta_{ij}P_i.$$

If we define

$$F_{ij} = f_{ij} + \sum_{r=m+1}^{\ell} \delta_{ir} f_{rj},$$

then the Euler identity can be rewritten as

$$(*) \qquad d_i f_i = \sum_j F_{ij} t_j - \sum_{r=m+1}^{\ell} d_r \delta_{ir} f_{rj}.$$

This follows from the sequence of identities

$$\begin{aligned} d_i f_i = \sum_j f_{ij} t_j &= \sum_j \left[F_{ij} - \sum_{r=m+1}^{\ell} \delta_{ir} f_{rj} \right] t_j \\ &= \sum_j F_{ij} t_j - \sum_j \left[\sum_{r=m+1}^{\ell} \delta_{ir} f_{rj} \right] t_j \\ &= \sum_j F_{ij} t_j - \sum_{r=m+1}^{\ell} \delta_{ir} \left[\sum_j f_{rj} t_j \right] \\ &= \sum_j F_{ij} t_j - \sum_{r=m+1}^{\ell} \delta_{ir} (d_r f_r). \end{aligned}$$

As in Part I, it now suffices to prove:

Lemma B *$F_{ij} \in$ the ideal $(f_1, \ldots, f_\ell) \subset S$.*

Proof The proof of Lemma B is analogous to Lemma A. First of all, we can expand

(i) $F_{ij} = \sum_k \rho_{ijk} e_k$.

Secondly, by differentiating P, we have

(ii) $\sum_{i=1}^m P_i F_{ij} = 0$.

If we substitute (i) into (ii), we obtain the identities

(iii) $\sum_{i=1}^m P_i \rho_{ijk} = 0$.

The minimality of $\{P_1, \ldots, P_m\}$ as a set of generators of $(P_1, \ldots, P_\ell)$ then forces $\deg \rho_{ijk} > 0$ whenever $\rho_{ijk} \neq 0$. ■

18-5 G as a pseudo-reflection group

In this section, we complete the proof of Theorem 18-1. We shall prove:

Proposition *If R is a polynomial algebra, then $G \subset \mathrm{GL}(V)$ is a pseudo-reflection group.*

The proof is a counting argument. Suppose

$$R = \mathbb{F}[x_1, \ldots, x_n], \quad \text{where } d_i = \deg x_i.$$

Let $H =$ the subgroup of G generated by the pseudo-reflections of G. Since $|H|$ divides $|G|$, we have that char $\mathbb{F}$ does not divide $|H|$. Since we have already proved that the invariants of a pseudo-reflection group are polynomial when the order of the group is prime to char $\mathbb{F}$, we can write

$$S^H = \mathbb{F}[y_1, \ldots, y_n].$$

If we let $e_i = \deg y_i$, and arrange the integers $\{d_1, \ldots, d_n\}$ and $\{e_1, \ldots, e_n\}$ so that

$$d_1 \leq d_2 \leq \cdots \leq d_n \quad \text{and} \quad e_1 \leq e_2 \leq \cdots \leq e_n,$$

then they satisfy two relations

(i) $d_i \geq e_i$ for all i.

For, since $R = S^G \subset S^H$, $d_i < e_i$ implies that each of $\{x_1, \ldots, x_i\}$ can be written as polynomials in $\{y_1, \ldots, y_{i-1}\}$. This would mean that $\{x_1, \ldots, x_i\}$ would not be algebraically independent, a contradiction.

(ii) $\prod_{i=1}^n d_i = \prod_{i=1}^n e_i$.

For both G and H contain the same number of pseudo-reflections. By Theorem A of §17-4, the number of pseudo-reflections in G and H is $\sum_{i=1}^n (d_i - 1)$ and $\sum_{i=1}^n (e_i - 1)$, respectively.

It follows from the relations (i) and (ii) that

$$d_i = e_i \quad \text{for all } i.$$

It then follows from Theorem A of §17-4 that

$$|G| = \prod_{i=1}^n d_i = \prod_{i=1}^n e_i = |H|.$$

Since $H \subset G$, it follows that $H = G$.

18-6 Invariants of Euclidean reflection groups

In this section, we demonstrate that, in the case of a Euclidean reflection group $W \subset \mathrm{GL}(\mathbb{E})$, the presence of a W-invariant inner product $(\_, \_)$ can be translated into invariant theory and used to prove several facts concerning the degrees of such reflection groups. We shall prove:

Proposition *Let $W \subset \mathrm{GL}(\mathbb{E})$ be a finite essential reflection group in Euclidean space with degrees $d_1 \leq d_2 \leq \cdots \leq d_\ell$. Then*

(i) $d_1 = 2$;
(ii) If W is an irreducible reflection group, then $d_i > 2$ for $i \geq 2$.

Remark 1: Assertion (i) can be strengthened to assert that, among the finite essential irreducible complex pseudo-reflection groups, Euclidean reflection groups are distinguished by the fact that $d_1 = 2$. See the list in Chapter 15 for an empirical verification of this fact.

Remark 2: Assertions (i) and (ii) will be used in Chapter 32 (see, in particular, Theorem 32-2C) to demonstrate that Coxeter elements of irreducible Euclidean reflection groups are characterized in a simple way by their eigenvalues. This in turn is part of a larger program in which invariant theory is used to analyze the eigenvalues of elements of pseudo-reflection groups. (See Chapters 33 and 34.)

Let V be a finite dimensional vector space over the field $\mathbb{F}$. We begin the proof of the proposition by observing that:

Lemma A *The elements from $S(V^*)$ of degree 2 can be identified with the quadratic forms on V.*

Proof Pick an element $q \in S(V^*)$ of degree 2. Then

$$q = \sum_{i=1}^{k} \alpha_i \beta_i, \quad \text{where } \alpha_i, \beta_i \in V^*.$$

If we consider q as a polynomial function $q\colon V \to \mathbb{R}$, then we have

$$q(x) = \sum_{i=1}^{k} \alpha_i(x)\beta_i(x) \quad \text{for any } x \in V.$$

We now show that, if we let

$$B(x, y) = q(x + y) - q(x) - q(y),$$

then B is bilinear and, so, q is a quadratic form. More precisely,

$$(*) \qquad B(x + y, z) = B(x, z) + B(y, z) \quad \text{for all } x, y, z \in V.$$

By the above definitions, and the linearity of α_i and β_i, we can write

$$B(x, y) = \sum_{i=1}^{k} [\alpha_i(x)\beta_i(y) + \alpha_i(y)\beta_i(x)].$$

The equality $B(x + y, z) = B(x, z) + B(y, z)$ then follows from

$$\begin{aligned} &\alpha_i(x + y)\beta_i(z) + \alpha_i(z)\beta_i(x + y) \\ &\quad = [\alpha_i(x) + \alpha_i(y)]\beta_i(z) + \alpha_i(z)[\beta_i(x) + \beta_i(y)] \\ &\quad = [\alpha_i(x)\beta_i(z) + \alpha_i(z)\beta_i(x)] + [\alpha_i(y)\beta_i(z) + \alpha_i(z)\beta_i(y)]. \end{aligned}$$

If there is an action of the group W on V, then we can easily extend the above lemma to:

Lemma B *The elements from $S(V^*)^W$ of degree 2 can be identified with the W-invariant quadratic forms on V.*

The proposition now follows.

Proof of Proposition By Remark 2 in §18-1, we can deal with the degrees $\{d_1^*, \dots, d_k^*\}$ of $S(\mathbb{E}^*)^G$. Regarding (i), asserting that $W \subset GL(\mathbb{E}^*)$ is essential is equivalent to asserting that $S_1(\mathbb{E}^*) = \mathbb{E}^*$ has no invariant elements. So $d_1^* \geq 2$. Also, the presence of a W-invariant inner product on $\mathbb{E}$ guarantees the existence of a nontrivial, W-invariant, quadratic form on $\mathbb{E}$. So $d_1^* \leq 2$.

Regarding (ii), it was explained in the Remark at the end of §2-4 that an irreducible essential reflection group is an irreducible representation. By Corollary B in Appendix C, if W acts irreducibly on $\mathbb{E}^*$, then any two W-invariant quadratic forms are scalar multiples of each other.

19 Modular invariants of pseudo-reflection groups

In this chapter, we discuss the modular case of invariant theory. We proved in Chapter 18 that, in the nonmodular case, a finite group $G \subset \mathrm{GL}(V)$ is a pseudo-reflection group if and only if the ring of invariants $S(V)^G$ is a polynomial algebra. This result is only partly true in the modular case. In §19-1, it will be shown that, if $S(V)^G$ is polynomial, then $G \subset \mathrm{GL}(V)$ is a pseudo-reflection group. However, the converse is not true. There are modular pseudo-reflection groups whose ring of invariants are not polynomial. Indeed, the ring of invariants of a pseudo-reflection group can be quite complex. On the other hand, if we pass from the ordinary invariants of a pseudo-reflection group to its "generalized invariants", then this invariant theory is much better behaved. These generalized invariants will be discussed in §19-2 and §19-3.

This chapter will not be needed in subsequent discussions. It is intended to give a succinct summary of the status of the results of Chapter 18 when passing to the modular case. Later chapters will return to the nonmodular case.

19-1 Polynomial rings of invariants

The arguments of this section are taken from Serre [1]. We shall prove:

***Theorem* (Serre)** *Let V be a finite dimensional vector space over a field $\mathbb{F}$. Given a finite group $G \subset \mathrm{GL}(V)$, if $S(V)^G$ is a polynomial algebra, then G is a pseudo-reflection group.*

This theorem generalizes one of the implications from Theorem 18-1 in that it does not use the hypothesis that char $\mathbb{F}$ does not divide $|G|$. The rest of this section will be devoted to the proof. The proof will omit some details. Notably, we shall cite certain results, such as the Purity of Branch Locus Theorem and Nakayama's Lemma, but not prove them.

We shall assume that $G \subset \mathrm{GL}(V)$ *is a finite group, where $S(V)^G$ is a polynomial algebra*. Let

$$H = \text{the subgroup of } G \text{ generated by the pseudo-reflections of } G.$$

Since pseudo-reflections of G are sent to other pseudo-reflections under conjugation, it follows that H is a normal subgroup of G. We want to show that $H = G$. The proof will proceed by a series of reductions. We shall consider, in turn,

(a) localization theory
(b) ramification theory
(c) inertia groups

and reduce the proof of $H = G$ to the assertion that certain (inertia) subgroups $I_G \subset G$ and $I_H (= H \cap I_G) \subset H$ satisfy $I_H = I_G$.

(a) Localization A general reference for localization is Atiyah-MacDonald [1]. For any integral domain A, we let $F(A)$ denote the quotient field of A. For any

integral domain A and any multiplicative set $\Gamma \subset A$, we can form

$$A_\Gamma = \text{the } \textit{localization} \text{ of } A \text{ with respect to } \Gamma.$$

If the finite group G acts on A and maps Γ to itself, then there is an induced action on A_Γ, and we have the identity

$$(*) \qquad (A_\Gamma)^G = (A^G)_{\Gamma^G}.$$

Notably, this gives the identity

$$(**) \qquad F(A)^G = F(A^G).$$

When $p \subset A$ is a prime ideal, and we localize A with respect to the multiplicative set $\Gamma = A - p$, we will write A_p, instead of A_Γ, and call

$$A_p = \text{the localization of } A \text{ at } p.$$

Observe that A_p is a *local ring*, i.e., it has a unique maximal ideal, namely the ideal pA_p generated by p.

Let $m \subset S$ be the maximal ideal generated by the homogeneous elements of positive degree. (This ideal is the way in which the grading of S is introduced into the argument.) Then

$$\begin{matrix} m^G \subset S^G \\ m^G = m \cap S^G \end{matrix} \quad \text{and} \quad \begin{matrix} m^H \subset S^H \\ m^H = m \cap S^H \end{matrix}$$

are maximal ideals consisting of the elements of positive degree in S^G and S^H, respectively. Let $Q \subset R$ be the local rings

$$Q = \text{the localization of } S^G \text{ at } m^G$$
$$R = \text{the localization of } S^H \text{ at } m^H.$$

Reduction I: It suffices to show that $Q = R$.

The action of G on S extends to an action on $F(S)$. By Galois theory, $H = G$ is equivalent to $F(S)^G = F(S)^H$. We also have the equivalences

$$F(Q) = F\big((S_m)^G\big) = F(S_m)^G = F(S)^G$$
$$F(R) = F\big((S_m)^H\big) = F(S_m)^H = F(S)^H.$$

Here S_m denotes the localization of S at m. In each line, the first equality follows from $(*)$ and the second from $(**)$.

(b) Ramification Theory To show that $Q = R$, we use ramification theory. The concept of ramification arises in the context of finite extensions $A \subset B$ of Noetherian, integrally closed domains. Recall from §16-3 that an element $x \in F(A)$ is *integral* over A if there exists a monic polynomial $f(t)$ with coefficients in A such that $f(x) = 0$. Given an integral domain A, we can form its quotient field $F(A)$. A is *integrally closed* if the only elements of $F(A)$ integral over A consist of A itself. Any unique factorization domain (UFD) is integrally closed because, given $a, b \in F(A)$, any integral relation

$$(a/b)^n + a_{n-1}(a/b)^{n-1} + \cdots + a_1(a/b) + a_0 = 0$$

can be converted to the relation

$$a^n + a_{n-1}a^{n-1}b + \cdots + a_1ab^{n-1} + a_0b^n = 0$$

in A. So any factor in b must be present in a. Thus b divides a and $a/b \in A \subset F(A)$. In particular, polynomial algebras $\mathbb{F}[x_1, \ldots, x_n]$ are UFD and, hence, integrally closed. Given $A \subset B$, a prime ideal $q \subset B$ *divides* the prime ideal $p \subset A$ (written $q|p$) if $q \cap A = p$. The ideal $pB \subset B$ can be decomposed

$$pB = \prod_{q|p} q^{e_q}$$

as a product of prime ideals. We say that the extension $A \subset B$ is *unramified at the prime ideal* $q \subset B$ if, letting $p = q \cap A$, we have $e_q = 1$ in the decomposition of pB and the finite extension $A/p \subset B/q$ is separable. The extension $A \subset B$ is unramified if $A \subset B$ is unramified at all prime ideals $q \subset B$.

We can apply the concepts of ramification to the extension $Q \subset R$. For, by the results of Chapter 16, this is a finite extension of Noetherian domains. Moreover, both Q and R are integrally closed. The integral closure of Q follows from the fact that S^G is polynomial and, hence, Q is a regular local ring. (See, for example, Chapter 11 of Atiyah-MacDonald [1].) The integral closure of R then follows from the fact that $Q \subset R$ is a finite extension.

Reduction II: It suffices to show that $Q \subset R$ is unramified.

If we consider the unique maximal ideals m_Q $(= m^G) \subset Q$ and m_R $(= m^H) \subset R$ it follows, from $Q \subset R$ being unramified, that

$$m_R = m_Q R.$$

Moreover, since $Q/m_Q = R/m_R = \mathbb{F}$, we also have the identity

$$R = Q + m_R.$$

Now, consider the Q module R/Q. By combining the above identities, we have

$$m_Q(R/Q) = (m_Q R + Q)/Q = (m_R + Q)/Q = R/Q.$$

It follows from Nakayama's Lemma (see Proposition 2.6 of Atiyah-MacDonald [1]) that $R/Q = 0$, and so $Q = R$.

Reduction III: It suffices to show that $Q \subset R$ is unramified at all minimal prime ideals $r \subset R$.

For, the Purity of Branch Locus theorem (see Nagata [1]) then implies that $Q \subset R$ is unramified.

(c) Inertia Groups We continue to work with ramification theory for finite extensions of Noetherian, integrally closed domains. Ramification can be measured by inertia groups. If $A \subset B$ is Galois with Galois group G (i.e., $A = B^G$), then, for any prime ideal $q \subset B$, we define the *inertia group*

$$I = \{\varphi \in G \mid \varphi \cdot q \subset q \text{ and } \varphi = 1 \text{ on } B/q\}.$$

The inertia subgroup measures ramification at q. As before, let $p = A \cap q$. We define $A/p \subset K \subset B/q$ by

$$K = \text{the maximal separable sub-extension of } A/p \subset B/q.$$

If we let

$$d_q = \text{the degree of } K \subset B/q,$$

then

$$|I| = d_q e_q.$$

In particular, if I is trivial, then $A \subset B$ is unramified at q.

We shall deal with the extension $Q \subset R$, which has Galois group G/H. We want to show that the extension is unramified at any *minimal prime ideal* $r \subset R$, i.e., any prime ideal $0 \neq r' \subseteq r$ must satisfy $r' = r$. In order to show that $Q \subset R$ is unramified at r, it suffices to show that the associated inertia group $I_{G/H} \subset G/H$ is trivial. Let

$$T = \text{the localization of } S \text{ at } m.$$

Then we have $Q \subset R \subset T$, where $Q \subset T$ and $R \subset T$ have Galois groups G and H, respectively. Pick a prime ideal $t \subset T$ such that

$$r = t \cap R.$$

Let

$$q = t \cap Q.$$

Then we have the inertia groups I_G, I_H, and $I_{G/H}$ of t, q and r, respectively. They satisfy the identity

$$I_{G/H} = I_G/I_H.$$

Therefore, we want to show that $I_H = I_G$. From the identity

$$I_H = I_G \cap H$$

it suffices to show that $I_G \subset H$. We shall prove a stronger result by showing that:

Proposition *Every nontrivial element of I_G is a pseudo-reflection on V.*

First of all, the action of G on V can be recovered from the action of G on T in the following fashion. We have the identity $V = m/(m^2)$ and the action of G on T induces an action of G on $V = m/(m^2)$. This action agrees with the given action of G on V. Equivalently, we are given a homomorphism

$$\mathcal{E}\colon G \to \mathrm{GL}(V),$$

which agrees with the given inclusion $G \subset \mathrm{GL}(V)$.

We shall show that, for each $\varphi \in I_G$, if $\mathcal{E}(\varphi) \neq 1$, then $\mathcal{E}(\varphi)$ is a pseudo-reflection. We have $t \subset m$.

Lemma A *The image of t in $V = m/(m^2)$ has dimension ≤ 1.*

Proof Given $x \in t$ such that $x \neq 0$ in $m/(m^2)$, then xT is a prime ideal of T because T is regular. More precisely, if we filter T by $\cdots \subset m^2 \subset m \subset T$ then the associated graded ring $\mathrm{gr}(T)$ satisfies

$$\mathrm{gr}(T) = k[x_1, \ldots, x_n],$$

where $\{x_i\}$ is an $\mathbb{F}$ basis of $m/(m^2)$. In particular, we can assume $x_n = x$. So $\mathrm{gr}(S/xS) = k[x_1, \ldots, x_n]$. In particular, S/xS is an integral domain. Since $xT \subset t$ is prime, we must have $xT = t$. Otherwise, t is not a minimal prime. ■

Finally, we have:

Lemma B *Let $\varphi\colon V \to V$ be a linear transformation of finite order and let $L \subset V$ be an one-dimensional subspace, invariant under φ, such that $\varphi = 1$ on V/L. Then either $\varphi = 1$, or φ is a pseudo-reflection.*

Proof By hypothesis, $V = \mathbb{F}x \oplus \mathbb{F}y \oplus U$, where

$$\varphi \cdot x = \xi x \quad \xi^n = 1$$

$$\varphi \cdot y = y + x$$

$$\varphi = 1 \text{ on } U.$$

(Here $L = \mathbb{F}x$.) Let

$$z = \xi x + (\xi - \xi^2)y.$$

Then $\varphi \cdot z = z$. So $\varphi = 1$ on the hyperplane $H = U + \mathbb{F}z$ and $\mathrm{rank}(\varphi - 1) \leq 1$. ■

By Lemma A, for each $\varphi \in I_G$, $\mathcal{E}(\varphi) \in \mathrm{GL}(V)$ satisfies the hypothesis of Lemma B. Hence, either $\mathcal{E}(\varphi) = 1$, or $\mathcal{E}(\varphi)$ is a pseudo-reflection.

19-2 Generalized invariants

We know from §19-1 that only pseudo-reflection groups can have a polynomial algebra as their ring of invariants. But not every pseudo-reflection group has polynomial invariants. A standard example of this phenomenon is the invariants of the Weyl group $W(F_4)$. Since this reflection group is defined over $\mathbb{Z}$, we can reduce mod p and get an $\mathbb{F}_p$ reflection group. It turns out that the mod 3 and mod 5 invariants of $W(F_4)$ are not polynomial. In particular, when $p = 3$ we have, by Toda [1],

$$\mathbb{F}_3[t_1, t_2, t_3, t_4]^{W(F_4)} = \mathbb{F}_3[x_4, x_8, x_{20}, x_{36}, x_{48}]/R,$$

where

$$R = \text{the ideal } (x_{20}^3 - x_4^3 x_{48} - x_8^3 x_{36} + x_4 x_8^2 x_{20}^2).$$

On the other hand, Kac and Peterson have demonstrated that, in a suitably modified and generalized version, the invariants of a pseudo-reflection group are "polynomial". The main references for their work are Kac-Peterson [1], [2] and Kac [1], as well as Neumann-Neusel-Smith [1]. They work with what they call the "generalized invariants" of a pseudo-reflection group. In all that follows, we shall be dealing with a finite pseudo-reflection group $G \subset \mathrm{GL}(V)$ for a finite dimensional vector space V over the field $\mathbb{F}_p$. Besides $S = S(V)$, we let

$$S_+ = \sum_{i \geq 1} S_i$$

$$I = \text{the ideal generated by } S_+^G = \sum_{i \geq 1} S_i^G.$$

The generalized invariants will be defined below. They form an ideal $J \subset S$ containing the ideal I. We shall demonstrate in §19-3 that J is always generated by a regular sequence. So $J = (x_1, \ldots, x_n)$, where $\{x_1, \ldots, x_n\}$ generates a polynomial subalgebra $\mathbb{F}_p[x_1, \ldots, x_n] \subset S(V)$. However, the choice of $\{x_1, \ldots, x_n\}$ is not canonical. And, thus, $\mathbb{F}_p[x_1, \ldots, x_n]$ is not canonical. Only the ideal $J = (x_1, \ldots, x_n)$ is canonical.

To define the generalized invariants, we use the Δ operations defined as in §18-2. For each pseudo reflection $s\colon V \to V$, we have an operation

$$\Delta\colon S \to S,$$

which lowers degree by 1. The operation is defined in terms of $s\colon S \to S$. Choose $\alpha \in V \subset S$ such that $\mathrm{Im}(s - 1) = \mathbb{F}_p\alpha$. Then, for any x

$$(*) \qquad s \cdot x = x + \Delta(x)\alpha.$$

The multiplicative relation $s \cdot (xy) = (s \cdot x)(s \cdot y)$ then gives the relation

$$(**) \qquad \Delta(xy) = \Delta(x)y + (s \cdot x)\Delta(y).$$

So Δ is a *twisted derivation* (associated with G).

Definition: The *ideal of generalized invariants* is

$$J = \left\{ x \in S_+ \;\middle|\; \begin{array}{c} (\phi_o \Delta_1 \phi_1 \cdots \Delta_k \phi_k) \cdot x \in S_+ \text{ for all twisted derivations} \\ \Delta_1, \dots, \Delta_k \text{ and } \phi_o, \dots, \phi_k \in G \end{array} \right\}.$$

The ideal J is graded, i.e., $J = \bigoplus_{k \geq 0} J_k$, where $J_k = J \cap S_k$ for all k. Observe that J is invariant under the Δ operations as well as under G. Moreover, we can characterize J as the largest such invariant ideal.

In many cases, there exists an alternative definition of J that makes the term "generalized invariants" even more appropriate. Define a sequence of ideals

$$\{0\} = J(0) \subset J(1) \subset \cdots \subset J(k) \subset J(k+1) \subset \cdots$$

of S, where

$$J(k+1) = \text{the ideal generated by } \{x \in S_+ \mid \phi \cdot x = x \text{ in } S/J(k) \text{ for all } \phi \in G\}.$$

Observe that $J(1) = (S_+^G) = I$. The union $\bigcup_{k \geq 0} J(k)$ is called the *ideal of stable invariants.* We always have:

Lemma A $J \subset \bigcup_{k \geq 0} J(k)$.

Proof Decompose J into its homogeneous components $J = \bigoplus_{k \geq 0} J_k$. We can prove, by induction on k, that $J_k \subset J(k)$.

Case $k = 1$ If $x \in J_1$, then $\Delta(x) = 0$ for all twisted derivations associated to G. Consequently $s \cdot x = x$ for all pseudo-reflections s. So $x \in S_+^G$.

General Case k If $x \in J_k$, then $\Delta_1 \cdots \Delta_k(x) = 0$ for any choice of twisted derivation $\{\Delta_1, \dots, \Delta_k\}$ associated to G. By induction, $\Delta(x) \in J(k-1)$ for every such twisted derivation. Consequently, $s \cdot x = x$ in $S/J(k-1)$ for all pseudo-reflections s. Thus $x \in J(k)$. ■

In general $J \neq \bigcup_{k \geq 0} J(k)$. However:

Lemma B *If $G \subset \mathrm{GL}(V)$ is a pseudo-reflection group in which all pseudo-reflections are of order prime to p, then $J = \bigcup_{k \geq 0} J(k)$.*

Proof We shall show, by induction on k, that $J(k) \subset J$. Since $J(1) = I \subset J$, the case $k = 1$ follows. Assume $J(k) \subset J$ and consider $J(k+1)$. Pick an element $x \in J(k+1)$. In order to show that $J(k+1) \subset J$, it suffices to consider the generators of $J(k+1)$. So we can assume that $\phi \cdot x \equiv x \big(\text{mod } J(k)\big)$ for all $\phi \in G$. First of all, $x \in J(k+1)$ and $J(k) \subset J$ tells us that

$$(*) \qquad \phi \cdot x \equiv x \text{ (mod } J) \quad \text{for all } \phi \in G.$$

Secondly, we have

$$(**) \qquad \Delta(x) \in J \quad \text{for every twisted derivation } \Delta.$$

To see this, choose the reflection s such that $s \cdot x = x + \Delta(x)\alpha$. We have $s^N = 1$, where $N \neq 0$ in $\mathbb{F}$. In particular $s \cdot \alpha = \xi\alpha$, where $\xi^N = 1$.

$$\Delta(s + s^2 + \cdots + s^N) = 0.$$

To prove this, let H be the hyperplane such that $s|_H = 1$. So $V = H \oplus \mathbb{F}\alpha$. We have

$$(s + s^2 + \cdots + s^N)\alpha = (\xi + \xi^2 + \cdots + \xi^N)\alpha = 0.$$

Also, for $y \in H$ we have $\Delta(y) = 0$. So

$$\Delta(s + s^2 + \cdots + s^N)(y) = \Delta(Ny) = N\Delta(y) = 0.$$

To prove $(**)$, it suffices to show $N\Delta(x) \in J$. We have

$$N\Delta(x) = N\Delta(x) - \Delta(s + \cdots + s^N)(x) = \Delta\Big(\sum_{i=1}^{N} x - s^i \cdot x\Big)$$

and

$$\Delta\Big(\sum_{i=1}^{N} x - s^i \cdot x\Big) \in \Delta(J) \subset J.$$

Notably, it follows from $(*)$ that $x - s^i \cdot x \in J$ for each i and, hence, that $\Delta(\sum_{i=1}^{N} x - s^i \cdot x) \in \Delta(J)$.

We can use $(*)$ and $(**)$ to force $x \in J$ because it follows from $(*)$ and $(**)$ that, if $x \notin J$, then J can be expanded to a bigger ideal of S_+ that is invariant under the elements of G as well as the Δ operators. This contradicts the fact that J is the maximal ideal of S_+ satisfying such an invariance property. So $x \in J$. ■

19-3 Regular sequences

In this section, we continue to discuss the ideal of generalized invariants.

Definition: Let S be a commutative Noetherian ring with identity. $\{x_1, \ldots, x_r\} \subset S$ is a *regular sequence* or S sequence if, for each $1 \leq i \leq r$, x_i is not a zero divisor in the quotient ring $S/(x_1, \ldots, x_{i-1})$.

Let V be a finite dimensional vector space over the field $\mathbb{F}$, and let $G \subset \mathrm{GL}(V)$ be a finite pseudo-reflection group. In this section we shall prove:

***Proposition* (Kac-Peterson)** *The ideal of generalized invariants $J \subset S(V)$ is generated by a regular sequence.*

The proof of the proposition will be in two steps.

(a) J/J^2 is a free S/J module.
(b) J is generated by a regular sequence.

Part (i) involves the explicit definition of J. In particular, the Δ operations are used in the proof. Part (ii) follows from part (i). The argument is much more general and can be done at the level of Noetherian local rings. We shall not provide all the details in part (ii).

Part (a) First of all, we choose the generators of J. Consider J as a S module. As before, let $S_+ = \sum_{i>0} S_i$. Then the module of indecomposables

$$Q(J) = J/(S_+J)$$

is a $S/S_+ = \mathbb{F}$ vector space and any set $\{x_1, \ldots, x_r\}$ projecting to a basis of $Q(J)$ generates J as an S module. So $\{x_1, \ldots, x_r\}$ generates J/J^2 as an S/J module. Freeness follows from

Lemma A *If $\alpha_1 x_1 + \cdots + \alpha_r x_r \in J^2$, then $\alpha_i \in J$ for each i.*

Proof Suppose there exists a relation

$$(*) \qquad \alpha_1 x_1 + \cdots + \alpha_r x_r \in J^2.$$

We want to show $(\phi_o \Delta_1 \phi_1 \cdots \Delta_k \phi_k) \cdot \alpha_i \in S_+$ for all choices of twisted derivations $\{\Delta_1, \ldots, \Delta_k\}$ associated with G and $\phi_o, \ldots, \phi_k \in G$. The proof is by induction on k. We call k the *height* of the element $\varphi = \phi_o \Delta_1 \phi_1 \cdots \Delta_k \phi_k$. The height zero case is obvious. If we apply φ to both sides of the relation $(*)$, then we obtain a relation of the form

$$(**) \qquad (\varphi \cdot \alpha_1)(\phi \cdot x_1) + \cdots + (\varphi \cdot \alpha_r)(\phi \cdot x_r) + \sum_i (\varphi' \cdot \alpha_i)(\varphi'' \cdot x_i) \in J^2,$$

where $\phi = \phi_o \phi_1 \cdots \phi_k$ and height $\varphi' < k$. Here we are using the twisted derivation property: $s \cdot (xy) = \Delta(x)y + (s\cdot)(x)\Delta(y)$. It follows from $(**)$ that

$$(\varphi \cdot \alpha_1)(\phi \cdot x_1) + \cdots + (\varphi \cdot \alpha_r)(\phi \cdot x_r) \in J^2.$$

Applying ϕ^{-1}, we have

$$(\phi^{-1}\varphi \cdot \alpha_1)x_1 + \cdots + (\phi^{-1}\varphi \cdot \alpha_r)x_r \in J^2 \subset S_+J.$$

Since $\{x_1, \ldots, x_r\}$ are linearly independent in $Q(J) = J/(S_+J)$, it follows that $\phi^{-1}\varphi \cdot \alpha_i \in S_+$ for each i. Thus $\alpha_i \in S_+$ as well. ■

Part (b) The argument that J is generated by an S sequence is based on the work of Vasconcelos [1]. The concept of *projective dimension* is employed in this argument. We shall not attempt to explain this concept. Rather, we refer the reader to Chapter 4 of Weibel [1] for a discussion.

Let R be a local ring with unique maximal ideal $m \subset R$. An ideal $I \subset R$ is generated as an R module by any subset projecting to an $\mathbb{F} = R/m$ basis of $Q(I) = I/mI$. Any such set is called a *minimal generating set* of I.

Lemma B **(Vasconcelos)** *If R is a local ring, and $I \subset R$ is an ideal of finite projective dimension where I/I^2 is R/I free, then I is generated by an R-sequence. Moreover, any minimal generating set of I is such a sequence.*

Proof We shall only sketch the proof. Write $I/I^2 = (R/I)^k$. By a result of Auslander-Buchsbaum [1], the finite projective dimension of I implies that there exists $0 \neq x \in I$, where x can be chosen to be one of the free generators of I/I^2 and x is not a zero divisor in R. Let

$$R^* = R/(x) \quad \text{and} \quad I^* = I/(x).$$

Then $I/(I^*)^2 = (R/I)^{r-1}$. Moreover, I^* is of finite projective dimension (over R^*). This is based on the decomposition $I/xI = (x)/xI \oplus I^*$, and the easily established fact that $\operatorname{proj\,dim}_R I = \operatorname{proj\,dim}_{R^*} I/xI$. We now repeat the above argument. However, the R sequence constructed above is a minimal generating set, since it provides an S/I basis of $I/(I^*)^2$.

It is easy to deduce that, if one minimal generating set of R is an R-sequence, then every minimal generating set is an R-sequence. ■

The local ring case of Lemma B can be applied to the graded ring S and the ideal $J \subset S$. Let

$$\widehat{S} = \prod_{j \geq 0} S_j, \quad \text{the formal completion of } S$$

$$\widehat{S}_+ = \prod_{j > 0} S_j.$$

If we write $S = \mathbb{F}[t_1, \ldots, t_n]$, then $\widehat{S} = \mathbb{F}[[t_1, \ldots, t_n]]$. We have $J \subset S \subset \widehat{S}$. Let

$$\widehat{J} = \widehat{S}_+ J.$$

It follows from Lemma A that $\widehat{J}/(\widehat{J})^2$ is $\widehat{S}/\widehat{J}$ free. Since $\widehat{S} = \mathbb{F}[[t_1, \ldots, t_n]]$ is regular, and $\widehat{J} \subset \widehat{S}$ is finitely generated, it follows that $\widehat{J}$ is of finite projective dimension. So we can apply Lemma B to $\widehat{J}$. Now any minimal generating set of J is also a minimal generating set of $\widehat{J}$. So the elements form a regular sequence in $\widehat{S}$ (by Lemma B) and, hence, in S as well.

VI Skew invariants

The next three chapters will study skew invariants and their role in the invariant theory of pseudo-reflection groups. In Chapter 20, we introduce skew invariants and explain their relation to ordinary invariants. In particular, we demonstrate that the skew invariants are a free module over the ring of ordinary invariants. In Chapter 21, the important concept of the Jacobian of a pseudo-reflection group is discussed. In Chapter 22, we define the extended ring of invariants of a finite group and prove Solomon's theorem describing the structure of this ring in the case of pseudo-reflection groups.

The results of these chapters are preparation for the continued study of invariant theory. In particular, they are used in later chapters to further explore the relation between pseudo-reflection groups and the usual ring of invariants.

20 Skew invariants

This chapter introduces the skew invariants of pseudo-reflection groups. In particular, it is shown that the skew invariants have a very simple structure when considered as a module over the ordinary invariants.

20-1 Skew invariants

Let V be a finite dimensional vector space over the field $\mathbb{F}$ and *let $G \subset \mathrm{GL}(V)$ be a finite nonmodular pseudo-reflection subgroup*, i.e., a finite pseudo-reflection group such that $\operatorname{char}\mathbb{F}$ does not divide $|G|$. Besides the absolute invariants of G discussed in previous chapters, there is also the concept of relative invariants. Given a homomorphism

$$\chi\colon G \to \mathbb{F}^*,$$

we say that $f \in S(V)$ is a *relative invariant* (with respect to χ) if $\varphi \cdot f = \chi(\varphi) f$ for all $\varphi \in G$. In particular, the embedding $G \subset \mathrm{GL}(V)$ induces

$$\det\colon G \to \mathbb{F}^*.$$

Skew invariants are the relative invariants with respect to det inverse.

Definition: $f \in S(V)$ is a *skew invariant* if $\varphi \cdot f = (\det \varphi)^{-1} f$ for all $\varphi \in G$.

The name "skew" is motivated by the Euclidean case wherein a skew invariant must satisfy $s \cdot f = -f$ for all reflections. We should also remark that, if we work in $S(V^*)$ rather than $S(V)$, then skew invariants are defined by the property that $\varphi \cdot f = (\det \varphi) f$ for all $\varphi \in G$. The switch from $(\det \varphi)^{-1}$ to $(\det \varphi)$ when passing from $S(V)$ to $S(V^*)$ is based on the identity $\langle \varphi \cdot \alpha, x\rangle = \langle \alpha, \varphi^{-1} \cdot x\rangle$ holding for all $x \in V$ and $\alpha \in S(V^*)$.

Skew invariants will find various applications in subsequent chapters. In particular, the skew invariants Ω and J (to be defined in §20-2 and §21-1) will turn out to play a major role in understanding the ordinary invariants of G.

Example: Let $\Delta = \{\epsilon_i - \epsilon_j\}$ be the A_ℓ root system as given in §2-3. Then the Van der Monde determinant

$$\prod_{i<j} (\epsilon_i - \epsilon_j) = \det \begin{bmatrix} 1 & \epsilon_\ell & \cdots & \epsilon_\ell^\ell \\ 1 & \epsilon_{\ell-1} & \cdots & \epsilon_{\ell-1}^\ell \\ \vdots & \vdots & & \vdots \\ 1 & \epsilon_0 & \cdots & \epsilon_0^\ell \end{bmatrix}$$

is a skew invariant with respect to $W(\Delta) = \Sigma_{\ell+1}$. For $W(\Delta)$ is generated by the reflections $\{s_{\epsilon_i - \epsilon_j} = (i, j) \mid i < j\}$ and, since $s_{\epsilon_i - \epsilon_j}$ interchanges the i-th and j-th rows of the above matrix, it follows that $s_{\epsilon_i - \epsilon_j}$ is multiplication by -1 on $\prod_{i<j} (\epsilon_i - \epsilon_j)$.

We shall see that this example can be generalized to every pseudo-reflection group. We use the element $\Omega = \prod_s \alpha_s$ as defined in §20-2.

Just as the invariants $S(V)^G$ of G are characterized by the averaging operator $\mathrm{Av}(x) = \frac{1}{|G|}\sum_{\varphi\in G}\varphi\cdot x$, so the skew invariants are characterized by the skew operator

$$\mathcal{S}k\colon S(V) \to S(V)$$

$$\mathcal{S}k(x) = \frac{1}{|G|}\sum_{\varphi\in G}(\det\varphi)\varphi\cdot x.$$

More precisely, $\mathcal{S}k$ is a projection operator with image consisting of the skew invariants. These properties for $\mathcal{S}k$ are proved in a manner analogous to the proof given of the same properties for the operator Av (see Lemma 14-3). We need to establish two facts. First of all, it is obvious that $\mathcal{S}k(x) = x$ if x is a skew invariant. Secondly, $\mathcal{S}k(x)$ is a skew invariant for any x. This follows from the equalities

$$\begin{aligned}
\phi\cdot\mathcal{S}k(x) &= \frac{1}{|G|}\sum_{\varphi\in G}(\det\varphi)(\phi\varphi)\cdot x\\
&= (\det\phi)^{-1}\frac{1}{|G|}\sum_{\varphi\in G}(\det\phi\varphi)(\phi\varphi)\cdot x\\
&= (\det\phi)^{-1}\frac{1}{|G|}\sum_{\varphi\in G}(\det\varphi)\varphi\cdot x \quad \text{(re-indexing)}\\
&= (\det\phi)^{-1}\mathcal{S}k(x).
\end{aligned}$$

20-2 The element Ω

Continue to assume that V is a finite dimensional vector space over $\mathbb{F}$ and $G \subset \mathrm{GL}(V)$ *is a finite nonmodular pseudo-reflection group.* For each pseudo-reflection $s \in G$, we can choose $\alpha_s \in V$ and $\Delta_s\colon V_s \to \mathbb{F}$ so that

$$s\cdot x = x + \Delta_s(x)\alpha_s$$

for all $x \in V$. In particular, the element α_s is an exceptional eigenvector of s, i.e.,

$$s\cdot\alpha_s = \xi\alpha_s.$$

Consider $\alpha_s \in S_1(V) = V$ and form the element

$$\Omega = \prod_s \alpha_s$$

in $S(V)$. Then $0 \neq \Omega \in S_N(V)$, where $N =$ the number of pseudo-reflections in G. Since the elements $\{\alpha_s\}$ are only determined up to a constant multiple, it follows that the same is true for Ω.

Example: Given a finite reflection group $W \subset GL(\mathbb{E})$, where $\mathbb{E}$ is Euclidean space, pick any root system $\Delta \subset \mathbb{E}$ and consider the positive roots Δ^+ with respect to some fundamental system of Δ. We can then write

$$\Omega = \prod_{\alpha>0} \alpha.$$

The example $\prod_{i<j}(\epsilon_i - \epsilon_j)$ discussed in §20-1 provides an explicit case of this formula.

In the rest of this section, we prove two facts about Ω.

Proposition A *Ω is skew.*

Proposition B *Ω divides every skew invariant.*

Remark 1: We have already found it useful in Chapter 18 to consider $S(V)$ as a module over $S(V)^G$. It is easy to see that the skew invariants form a $S(V)^G$ submodule of $S(V)$. The above two propositions amount to asserting that the skew invariants of G form a free $S(V)^G$ module with Ω as generator.

Remark 2: We can prove similar results for all relative invariants (i.e., for every homomorphism $\chi\colon G \to \mathbb{F}^*$). We can construct an analogue of Ω and show that it satisfies analogues of the above propositions.

The proof of the above propositions will occupy the rest of this section. The argument will be broken down into three stages, consisting of two preliminary steps, followed by the proof of the propositions. The two preliminary stages are:

(I) Reformulate and simplify the decomposition $\Omega = \prod \alpha_s$ given above;
(II) Use this new formulation to study the action of G on Ω.

Step I: Reformulation of Ω The reformulation of Ω is based on the following two lemmas.

Lemma A *α_s and $\alpha_{s'}$ are multiples of each other if and only if s and s' have the same invariant hyperplanes.*

For each hyperplane $H \subset V$, let

$G_H =$ the subgroup of G generated by the pseudo-reflections having H as their invariant hyperplane.

Lemma B *For all H, G_H is a cyclic group.*

Granted the above lemmas, we can rewrite the element Ω. Let

$$o(H) = \text{the order of the cyclic group } G_H.$$

Because of Lemma A, we can choose α_s to be the same for all $s \in G_H$. We use α_H to denote this common eigenvector. Then

$$\Omega = \prod_H \alpha_H^{o(H)-1}$$

where H runs through the invariant hyperplanes of G.

Proof of Lemma A Let $K \subset G$ be the subgroup generated by s and s'. Then the fact that char $\mathbb{F}$ does not divide $|G|$ implies that char $\mathbb{F}$ does not divide $|K|$. So, by Maschke's theorem from Appendix B, the action of K on V is completely reducible.

First of all, suppose that $\mathbb{F}\alpha_s = \mathbb{F}\alpha_{s'}$ ($= L$, say). Since α_s and $\alpha_{s'}$ are eigenvectors of s and s', respectively, we know that L is invariant under K. Using Maschke's theorem, choose a hyperplane $H \subset V$ invariant under K such that $V = H \oplus L$. We claim that

$$H = \text{the invariant hyperplane of both } s \text{ and } s'.$$

Consider s. Any eigenvector of s projects in both H and L to an eigenvector (with the same eigenvalue). Consequently, since s is multiplication on L by a nontrivial root of unity, the invariant hyperplane of s (on which s is multiplication by 1) lies entirely within H. By comparing dimensions, this invariant hyperplane agrees with H.

Conversely, assume that s and s' have a common pointwise invariant hyperplane $H \subset V$. Choose a line $L \subset V$, invariant under K, such that $V = H \oplus L$. The exceptional eigenvectors, α_s and $\alpha_{s'}$, of s and s' cannot lie in H; so, arguing as above, they must lie in L. Hence they are multiples of each other. ∎

Proof of Lemma B As in the proof of Lemma A, we can decompose $V = H \oplus L$, where L is G_H invariant. Each element of G_H is multiplication on L by some n-th root of unity. So G_H is a cyclic group with order equal to the LCM of the n's. ∎

Step II: Action of G ***on*** Ω Now we study the action of G, first on the invariant hyperplanes $\{H\}$ and on the elements $\{\alpha_H\}$, and then on Ω. Given $\varphi \in G$, the map

$$G \to G$$
$$x \mapsto \varphi x \varphi^{-1}$$

sends pseudo-reflections to pseudo-reflections. Also, φ permutes the associated invariant hyperplanes. If $\varphi s \varphi^{-1} = s'$, then $\varphi \cdot H = H'$, where H and H' are the invariant hyperplanes of s and s'.

It follows from Lemma A that φ also permutes the elements $\{\alpha_H\}$ up to multiples of each other. If $\varphi \cdot H = H'$, then

$$\varphi \cdot \alpha_H = c\alpha_{H'}$$

for some $c \in \mathbb{F}$. These constants $\{c\}$ are not generally well defined, since we can always alter the elements $\{\alpha_H\}$ by scalar multiples. However, when we let $\varphi =$ the pseudo-reflection s, then the constants $\{c\}$ still satisfy important constraints.

First of all, there is one case when the constant c is well defined and easy to determine. Given a pseudo-reflection s from G with invariant hyperplane H_s, then α_{H_s} is an exceptional eigenvector for s. So:

Lemma C $s \cdot \alpha_{H_s} = (\det s)\alpha_{H_s}$.

Next, divide the invariant hyperplanes $\{H\}$ into their orbits under s. By the above lemma, one of the orbits consists of the single element $\{H_s\}$. We also have:

Lemma D *If $\{H_1, \ldots, H_k\}$ is not the orbit $\{H_s\}$, then*

$$s \cdot (\alpha_{H_1} \cdots \alpha_{H_k}) = \alpha_{H_1} \cdots \alpha_{H_k}.$$

Proof We can assume that the orbit is arranged so that

$$s \cdot H_1 = H_2, \ldots, \quad s \cdot H_{k-1} = H_k, \quad s \cdot H_k = H_1.$$

Consequently,

$$(*) \qquad \begin{cases} s \cdot \alpha_{H_i} = c_i \alpha_{H_{i+1}} & \text{for } 1 \leq i \leq k-1 \\ s \cdot \alpha_{H_k} = c_k \alpha_{H_1}. \end{cases}$$

It follows from $(*)$ that $s \cdot (\alpha_{H_1} \cdots \alpha_{H_k}) = (c_1 \cdots c_k)\alpha_{H_1} \cdots \alpha_{H_k}$. So, to prove the proposition, it suffices to show

$$c_1 \cdots c_k = 1.$$

It follows from $(*)$ that

$$(**) \qquad s^k \cdot \alpha_{H_i} = (c_1 \cdots c_k)\alpha_{H_i} \quad \text{for each } 1 \leq i \leq k.$$

If $s^k = 1$, we are done. Therefore, assume $s^k \neq 1$. We shall show that $c_1 \cdots c_k \neq 1$ leads to a contradiction. First of all, s^k is a pseudo-reflection. Secondly, it follows from $(**)$ that $\{\alpha_{H_1}, \ldots, \alpha_{H_k}\}$ are exceptional eigenvectors of s^k. Since all the exceptional eigenvectors of s^k lie in $\mathbb{F}\alpha_{H_s}$, it follows that all of $\{\alpha_{H_1}, \ldots, \alpha_{H_k}\}$ are multiples of α_{H_s}. By Lemma A, we have $H_1 = \cdots = H_k$ $(= H_s)$, which contradicts the assumption that $\{H_1, \ldots, H_k\}$ is not the orbit $\{H_s\}$. ■

Proof of Proposition A Lemma C implies that

$$s \cdot (\alpha_{H_s}^{o(H_s)-1}) = (\det s)^{-1} \alpha_{H_s}^{o(H_s)-1},$$

while Lemma D implies that

$$s \cdot \Big(\prod_{H \neq H_s} \alpha_H^{o(H)-1} \Big) = \prod_{H \neq H_s} \alpha_H^{o(H)-1}.$$

Proof of Proposition B We want to show that a skew polynomial f is divisible by $\alpha_H^{o(H)-1}$ for each reflecting hyperplane H of G. Since the $\{\alpha_H\}$ are relatively prime (see Lemma A), and since $S(V)$ is a unique factorization domain, it then follows that f is divisible by the product $\Omega = \prod_H \alpha_H^{o(H)-1}$.

For each H, pick a reflection $s\colon V \longrightarrow V$ of order $o(H)$ with H as its invariant hyperplane. By Lemma C, $s \cdot \alpha_H = (\det s)\alpha_H$. We can expand $t_1 = \alpha_H$ to a basis $\{t_1, \ldots, t_n\}$ of V by choosing elements from the invariant hyperplane H of s. Now $f \in S(V) = \mathbb{F}[t_1, \ldots, t_n]$. Since $s \cdot f = (\det s)^{-1} f$, while $s \cdot (t_1^{k_1} \cdots t_n^{k_n}) = (\det s)^{k_1}(t_1^{k_1} \cdots t_n^{k_n})$, we can expand f in terms of the monomials $t_1^{k_1} \cdots t_n^{k_n}$ where $k_1 = -1 \bmod o(H)$. In particular, $k_1 \geq o(H) - 1$.

20-3 The ring of covariants

This final section of this chapter provides the first indication of the important role played by the element Ω in invariant theory. It will be demonstrated in Chapters 23 to 26 that Ω is the key to understanding the structure of the ring of covariants of a pseudo-reflection group. Let V be a finite dimensional vector space over $\mathbb{F}$ and *let $G \subset \mathrm{GL}(V)$ be a finite nonmodular pseudo-reflection group.* In Chapter 18, we introduced and used the ring of covariants S/I, where

$$S = S(V), \quad \text{the symmetric algebra}$$

$$I = \text{the graded ideal of } S \text{ generated by the homogeneous elements from } S^G \text{ of positive degree.}$$

Notably, in §18-3 we proved that S is a free S^G module generated by any set of elements projecting to an $\mathbb{F}$ basis of S/I. It follows that the Poincaré series of S, S^G and S/I are related by

$$P_t(S) = P_t(S^G)P_t(S/I).$$

Moreover, the Poincaré series of S and S^G are

$$P_t(S) = \frac{1}{(1-t)^n} \quad \text{and} \quad P_t(S^G) = \prod_{i=1}^{n} \frac{1}{1-t^{d_i}},$$

where $n = \dim_{\mathbb{F}} V$ and $\{d_1, \ldots, d_n\}$ are the degrees of G. It follows that:

Theorem $P_t(S/I) = \prod_{i=1} \frac{1-t^{d_i}}{1-t} = \prod_{i=1}^{n}(1 + t + \cdots + t^{d_i - 1})$.

This Poincaré series identity tells us that

$$P_t(S/I) = t^N + \text{lower terms},$$

where $N = (d_1 - 1) + (d_2 - 1) + \cdots + (d_n - 1)$. So we have:

Proposition A

(i) $S/I = 0$ *in* $\deg > N$.
(ii) $S/I = \mathbb{F}$ *in* $\deg N$.

So S has exactly one S^G generator of degree $\geq N$. The next lemma determines that generator. Let Ω be the skew-invariant element in S defined in §20-2.

Proposition B $S/I = \mathbb{F}\Omega$ *in* $\deg N$.

Proof We want to show that

$$S = I \oplus \mathbb{F}\Omega \quad \text{in } \deg N.$$

To prove this equality, it suffices to show $\Omega \notin I$, since, by the above Poincaré series, $I \subset S$ has codimension 1 in degree N. Let $\mathcal{S}k\colon S \to S$ be the skew-invariant projection operator defined in §20-1. Since Ω is a skew invariant, it follows that

$$(*) \qquad \mathcal{S}k(\Omega) = \Omega.$$

On the other hand,

$$(**) \qquad I \subset \operatorname{Ker} \mathcal{S}k \quad \text{in } \deg \leq N.$$

For, given $x \in I$ of degree $\leq N$, we can write

$$x = \sum_i u_i f_i,$$

where $f_i \in S^G$ and $u_i \in S$ are homogeneous and $\deg u_i < N$. Then

$$\mathcal{S}k(x) = \sum_i \mathcal{S}k(u_i) f_i.$$

Now, $\mathcal{S}k = 0$ in $\deg < N$, since, by §20-2, any skew invariant must be divisible by Ω. In particular, $\mathcal{S}k(u_i) = 0$. So $\mathcal{S}k(x) = 0$. A comparison of $(*)$ and $(**)$ yields $\Omega \notin I_W$. ∎

21 The Jacobian

This chapter continues the study of the skew invariants of pseudo-reflection groups. In this chapter, we introduce the Jacobian of a pseudo-reflection group. We shall demonstrate that it is a skew invariant and, also, nontrivial. The Jacobian will be used extensively in subsequent chapters.

21-1 The Jacobian

Assume that V is a finite dimensional vector space over the field $\mathbb{F}$, and that $G \subset \mathrm{GL}(V)$ *is a finite nonmodular pseudo-reflection group*. To define the Jacobian, choose a basis $\{t_1, \ldots, t_n\}$ of V and write

$$S = S(V) = \mathbb{F}[t_1, \ldots, t_n].$$

The Jacobian of G is an element of $S(V)$. Any $y \in S$ can be written as a polynomial in $\{t_1, \ldots, t_n\}$. So we can define the formal derivatives $\{\frac{\partial y}{\partial t_1}, \ldots, \frac{\partial y}{\partial t_n}\}$ in the usual way. If we write

$$S(V)^G = \mathbb{F}[x_1, \ldots, x_n],$$

then we define the *Jacobian* as

$$J = \det \left[\frac{\partial x_i}{\partial t_j}\right]_{n \times n}.$$

The definition of J involves the choice of the elements $\{t_1, \ldots, t_n\}$ and the elements $\{x_1, \ldots, x_n\}$. In particular, we can alter the elements $\{t_1, \ldots, t_n\}$ and $\{x_1, \ldots, x_n\}$ by scalar multiples which, in turn, alters J by a scalar multiple. However, modulo scalar multiples, J is well defined. This will follow from the first proposition below.

In the rest of this chapter, we shall prove two facts about J. First of all, let

$$\Omega = \prod_H \alpha_H^{o(H)-1}$$

be the skew-invariant product defined in §20-2.

Proposition A *$J = \lambda\Omega$ for some $\lambda \in \mathbb{F}$.*

It follows from Proposition A that J is a skew invariant and well-defined up to scalar multiple. Actually, it is easy to see that J being a skew invariant is equivalent to Proposition A. We shall give a more "natural" proof of Proposition A in §22-2. At the moment, we give a shorter proof based on the argument given at the end of §20-2.

The other result to be proved in this chapter is that:

Proposition B *$J \neq 0$.*

Much of the chapter will be taken up with the proof of Proposition B.

Remark: The above propositions demonstrate that a great deal of information about a finite nonmodular pseudo-reflection group $G \subset GL(V)$ is given by its ring of invariants $S(V)^G \subset S(V)$. For, given

$$\mathbb{F}[x_1, \ldots, x_n] = S(V)^G \subset S(V) = \mathbb{F}[t_1, \ldots, t_n],$$

we can form the Jacobian J as above. By the above propositions, we have a nontrivial decomposition of the form

$$J = \lambda \prod \alpha^{e(\alpha)},$$

where $\alpha \in S_1(V) = V$. Since $S(V)$ is UFD, such a decomposition into linear terms is unique up to scalar multiplication.

By the discussion in §20-2, the reflections $s\colon V \to V$ belonging to G are those with the elements $\{\alpha\}$ as exceptional eigenvectors.

(i) In the case of a Euclidean reflection group G, the elements $\{\alpha\}$ completely determine the group G. This is because of the presence of an inner product. Given α, let H be the hyperplane that is the orthogonal complement to $\mathbb{R}\alpha$. Thus for each α, there is a unique reflection s satisfying $s \cdot \alpha = -\alpha$ and $s|_H =$ the identity. Since G is generated by reflections, it is also completely determined.

(ii) In the general case of pseudo-reflection groups, the elements $\{\alpha\}$ only provide partial information about the group. For, given α, there is not a unique pseudo-reflection with α as the exceptional eigenvector. Notably, there is the far-from-unique choice of the invariant hyperplane H serving as the complement to $\mathbb{F}\alpha$.

21-2 The proof of Proposition A

The proof is analogous to the proof of Proposition 20-2B. We shall be using the notation from §20-2. For each reflecting hyperplane $H \subset V$ of G, pick a pseudo-reflection $s\colon V \to V$ of order $o(H)$ having H as its invariant hyperplane. By Lemma 20-2C,

$$s \cdot \alpha_H = (\det s)\alpha_H.$$

Expand $t_1 = \alpha_H$ to a basis $\{t_1, \ldots, t_n\}$ of V by choosing elements from the invariant hyperplane of $s\colon V \to V$. Given $f \in S(V)^G = \mathbb{F}[t_1, \ldots, t_n]^G$, then f can be expanded in terms of the monomials $t_1^{k_1} \cdots t_n^{k_n}$, where $k_1 \equiv 0 \bmod o(H)$. For

$$s \cdot f = f,$$

whereas

$$s \cdot (t_1^{k_1} \cdots t_n^{k_n}) = (\det s)^{k_1}(t_1^{k_1} \cdots t_n^{k_n}).$$

Thus f is divisible by $t_1^{o(H)}$ and $\frac{\partial f}{\partial t_1}$ is divisible by $t_1^{o(H)-1}$. So the first column of $[\frac{\partial x_i}{\partial t_j}]_{n\times n}$ is divisible by $t_1^{o(H)-1}$ and J is as well.

Since J is divisible by $\alpha_H^{o(H)-1}$ for each reflecting hyperplane $H \subset V$ of G, and since the linear forms $\{\alpha_H\}$ are relatively prime (see Lemma 20-2A), it follows that J is divisible by their product (for S is UFD). But both J and Ω have the same degree because

$$\deg \Omega = \text{the number of reflections in } G,$$

while

$$\deg J = (d_1 - 1) + \cdots + (d_n - 1),$$

where $\{d_1, \ldots, d_n\}$ are the degrees of G. So, by Corollary 18-1, $\deg \Omega = \deg J$. The proposition now follows. ■

21-3 The proof of Proposition B

The proof will follow the argument given in Benson [1]. Let $F(S)$ be the quotient field of S. We can prove the proposition by showing that, when we work over $F(S)$, then the matrix $[\frac{\partial x_i}{\partial t_j}]_{n\times n}$ has an inverse and, hence, its determinant is nonzero.

As already mentioned, we can define in the usual formal way, for $S = \mathbb{F}[t_1, \ldots, t_n]$, the partial derivatives

$$\frac{\partial}{\partial t_i} : S \to S.$$

Similarly, we can restrict to the subring $R = \mathbb{F}[x_1, \ldots, x_n]$ and define the partial derivative $\frac{\partial}{\partial x_i} : R \to R$.

What is not so obvious is that, if we work in $F(S)$, then we can extend the domain of definition of $\frac{\partial}{\partial x_i}$ from R to S, and the resulting extended partial derivatives

$$\frac{\partial}{\partial x_i} : S \to F(S)$$

are related to the standard partial derivatives $\frac{\partial}{\partial t_i} : S \to S$ by a chain rule.

Chain Rule:

$$\frac{\partial z}{\partial x_j} = \sum_k \frac{\partial z}{\partial t_k}\frac{\partial t_k}{\partial x_j} \quad \text{for any } z \in S.$$

This chain rule relation is the key to proving that the matrix $[\frac{\partial x_i}{\partial t_j}]_{n\times n}$ has an inverse. It implies that the matrix $[\frac{\partial t_i}{\partial x_j}]_{n\times n}$is the desired inverse. Just substitute $z = x_i$ into the above formula and we obtain the identity

$$\sum_k \frac{\partial x_i}{\partial t_k}\frac{\partial t_k}{\partial x_j} = \delta_{ij}.$$

Thus the proposition will be proven once the extended partial derivatives are defined and it is verified that they satisfy the chain rule.

21-4 Extended partial derivatives

If we pass from S to its quotient field $F(S)$, then we can give a recipe for defining, in $F(S)$, the *partial derivatives* $\frac{\partial z}{\partial x_1}, \ldots, \frac{\partial z}{\partial x_n}$ for each $z \in S$. We define $\frac{\partial z}{\partial x_i}$ by working backwards. We assume that we can define $\frac{\partial z}{\partial x_i}$ and show that a certain equation involving $\frac{\partial z}{\partial x_i}$ must hold; this equation is then used to define $\frac{\partial z}{\partial x_i}$.

Assume that

$$\frac{\partial}{\partial x_i} : S \to F(S)$$

is defined on S and that it acts like a derivative. Consider $z \in S$. Let $f \in R[T]$ be the minimal polynomial for z over R. So $f(z) = 0$. Since $R \subset S$ is separable, we also know that

$$\frac{\partial f}{\partial T}(z) \neq 0.$$

If we differentiate the equation

$$f(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0 = 0$$

with respect to x_i, then we obtain the equation

$$(*) \qquad \frac{\partial f}{\partial T}(z)\frac{\partial z}{\partial x_i} = -\frac{\partial f}{\partial x_i}(z),$$

where, on the right hand side, we are differentiating the coefficients of $f(z)$. Observe also that the "coefficients" $\frac{\partial f}{\partial T}(z)$ and $\frac{\partial f}{\partial x_i}(z)$ of the equation are standard formal derivatives that we already know how to determine. Since we are working in the field $F(S)$, this identity can now be solved for $\frac{\partial z}{\partial x_i}$. So equation $(*)$ gives a way of determining $\frac{\partial z}{\partial x_i}$ from known data. And this is how we proceed. Namely, we shall treat $\frac{\partial z}{\partial x_i}$ as being defined through the above equation. The resulting map

$$\frac{\partial}{\partial x_i} : S \to F(S)$$

represents an extension of the partial derivative

$$\frac{\partial}{\partial x_i} : R \to R.$$

In other words, given $z \in R \subset S$, then $\frac{\partial z}{\partial x_i}$, as defined above in $(*)$, is the usual formal derivative on R. The point is that the minimal polynomial f over R for such z is linear. Indeed, $f = T - z$.

The above partial derivatives satisfy the chain rule given in §21-3. The next section will be devoted to proving this fact. Before passing to the proof (in the next section), we give a very simple example demonstrating the above definitions, as well as the chain rule.

Example: The group $\mathbb{Z}/2\mathbb{Z}$ acts on the plane $\mathbb{R}^2 = \{(t_1, t_2)\}$ by permuting coordinates. Thus it also acts on the polynomial ring $S = \mathbb{R}[t_1, t_2]$ by permuting the terms $\{t_1, t_2\}$. The polynomials

$$x_1 = t_1 + t_2$$

$$x_2 = t_1 t_2$$

are fixed under this action and generate the ring of invariants. Namely, we have

$$R = S^{\mathbb{Z}/2\mathbb{Z}} = \mathbb{R}[t_1, t_2]^{\mathbb{Z}/2\mathbb{Z}} = \mathbb{R}[x_1, x_2].$$

Clearly, we have the four partial derivatives

$$(**) \qquad \frac{\partial x_1}{\partial t_1} = 1, \quad \frac{\partial x_1}{\partial t_2} = 1, \quad \frac{\partial x_2}{\partial t_1} = t_2, \quad \frac{\partial x_2}{\partial t_2} = t_1.$$

To calculate the partial derivatives $\frac{\partial t_k}{\partial x_j}$, we use the fact that the minimal polynomial over $F(R)$ of both t_1 and t_2 is

$$f(T) = (T - t_1)(T - t_2) = T^2 - x_1 T + x_2.$$

We have $\frac{\partial f}{\partial T}(T) = 2T - x_1$, $\frac{\partial f}{\partial x_1}(T) = -T$ and $\frac{\partial f}{\partial x_2}(T) = 1$. Hence

$$\frac{\partial f}{\partial T}(t_1) = t_1 - t_2 \quad \text{and} \quad \frac{\partial f}{\partial T}(t_2) = t_2 - t_1$$

$$\frac{\partial f}{\partial x_1}(t_1) = -t_1 \quad \text{and} \quad \frac{\partial f}{\partial x_1}(t_2) = -t_2$$

$$\frac{\partial f}{\partial x_2}(t_1) = \frac{\partial f}{\partial x_2}(t_2) = 1.$$

(In the first case, we use the identity $x_1 = t_1 + t_2$.) It now follows from $(*)$ that the partial derivatives $\frac{\partial t_k}{\partial x_j}$ are as follows:

$$(***) \qquad \begin{aligned} \frac{\partial t_1}{\partial x_1} &= \frac{t_1}{t_1 - t_2}, & \frac{\partial t_1}{\partial x_2} &= \frac{-1}{t_1 - t_2} \\ \frac{\partial t_2}{\partial x_1} &= \frac{t_2}{t_2 - t_1}, & \frac{\partial t_2}{\partial x_2} &= \frac{-1}{t_2 - t_1}. \end{aligned}$$

By substituting these values, we can verify all four possible cases of the chain rule

$$\sum_k \frac{\partial x_i}{\partial t_k} \frac{\partial t_k}{\partial x_j} = \delta_{ij}$$

stated in §21-3. For example,

$$\frac{\partial x_2}{\partial t_1}\frac{\partial t_1}{\partial x_2} + \frac{\partial x_2}{\partial t_2}\frac{\partial t_2}{\partial x_2} = (t_2)\left(\frac{-1}{t_1 - t_2}\right) + (t_1)\left(\frac{-1}{t_2 - t_1}\right) = 1.$$

21-5 The chain rule

We explained in §21-4 how to define the "partial derivatives" $\frac{\partial z}{\partial x_j}$, $\frac{\partial z}{\partial t_k}$ and $\frac{\partial t_k}{\partial x_j}$ by using minimal polynomials. In this section, we want to prove that they are related via:

Chain Rule Lemma

$$\frac{\partial z}{\partial x_j} = \sum_k \frac{\partial z}{\partial t_k}\frac{\partial t_k}{\partial x_j} \quad \textit{for any } z \in S.$$

We shall first establish a relation among the various minimal polynomials, and then use it to establish the lemma. The relation between the polynomials will depend on the following.

Lemma *Let $\mathbb{F} \subset \mathbb{F}(\alpha_1, \ldots, \alpha_n)$ be a finite separable extension and, for each $1 \leq i \leq n$, let $f_i \in \mathbb{F}[T]$ be the minimal polynomial of α_i over $\mathbb{F}$. Suppose that $\{\alpha_1, \ldots, \alpha_n\}$ are algebraically dependent over $\mathbb{F}$, and that $g \in \mathbb{F}[X_1, \ldots, X_n]$ is a polynomial satisfying*

$$g(\alpha_1, \ldots, \alpha_n) = 0.$$

Then there exists a polynomial $h \in \mathbb{F}[X_1, \ldots, X_n]$ such that

(i) $h(\alpha_1, \ldots, \alpha_n) \neq 0$;
(ii) gh belongs to the ideal of $\mathbb{F}[X_1, \ldots, X_n]$ generated by $\{f_1(X_1), \ldots, f_n(X_n)\}$.

Proof We proceed by induction on n. The $n = 1$ case is straightforward. We can let $h = 1$. This follows from the standard fact that the minimal polynomial $m \in \mathbb{F}[T]$ of α_1 divides any polynomial $g \in \mathbb{F}[T]$ satisfying $g(\alpha_1) = 0$.

For the general case, consider the extensions $\mathbb{F} \subset \mathbb{F}(\alpha_1) \subset \mathbb{F}(\alpha_1, \ldots, \alpha_n)$. If we work in the polynomial ring $\mathbb{F}(\alpha_1)[T]$, then the polynomials $f_2, \ldots, f_n$ factorize as

(1) $f_i = f_i' f_i''$, where $f_i', f_i'' \in \mathbb{F}(\alpha_1)[T]$ and

$$f_i' = \text{the minimal polynomial of } \alpha_i \text{ over } \mathbb{F}(\alpha_1)$$
$$f_i''(\alpha_i) \neq 0.$$

Let

$$g' = g(\alpha_1, X_2, \ldots, X_n) \in \mathbb{F}(\alpha_1)[X_2, \ldots, X_n].$$

By the induction hypothesis, there exists $h' \in \mathbb{F}(\alpha_1)[X_2, \ldots, X_n]$ such that

(2) $h'(\alpha_2, \ldots, \alpha_n) \neq 0$;
(3) $g'h'$ belongs to the ideal of $\mathbb{F}[X_2, \ldots, X_n]$ generated by $\{f_2'(X_2), \ldots, f_n'(X_n)\}$.

If we let

$$H = f_2'(X_2) \cdots f_n'(X_n)h',$$

then it follows from (2), (3) and (4) that

(4) $H(\alpha_2, \ldots, \alpha_n) \neq 0$;
(5) $g'H$ belongs to the ideal of $\mathbb{F}(\alpha_1)[X_2, \ldots, X_n]$ generated by $\{f_2(X_2), \ldots, f_n(X_n)\}$.

By using the identity $\mathbb{F}(\alpha_1) = \mathbb{F}(X_1)/\big(f_1(X_1)\big)$, the lemma follows. ■

We shall apply the lemma to the separable extension $F(R) \subset F(S)$. We can write $F(S) = F(R)(t_1, \ldots, t_n)$. Given $z \in S$, we can write z as a polynomial in $\{t_1, \ldots, t_n\}$. Let

$$g \in \mathbb{F}[T_1, \ldots, T_n, Z]$$

be the polynomial expressing this relation. So $g(t_1, \ldots, t_n, z) = 0$. If

$$f, f_1, \ldots, f_n \in F(R)[T]$$

are the minimal polynomials of $z, t_1, \ldots, t_n$, respectively, over $F(R)$, then it follows from the above lemma that there exists

$$h \in F(R)[T_1, \ldots, T_n, Z]$$

such that

(i) $h(t_1, \ldots, t_n, z) \neq 0$;
(ii) gh belongs to the ideal of $F(R)[T_1, \ldots, T_n, Z]$ generated by

$$\{f(Z), f_1(T_1), \ldots, f_n(T_n)\}.$$

So we have, in $F(R)[T_1, \ldots, T_n, Z]$, an identity of the form

$$(*) \qquad gh = \alpha f + \sum_j \alpha_j f_j.$$

The coefficients of α, α_i, h lie in $F(R) = \mathbb{F}(x_1, \ldots, x_n)$. By clearing denominators, we can assume that the coefficients actually belong to the polynomial ring $R = \mathbb{F}[x_1, \ldots, x_n]$. Replacing $\mathbb{F}[x_1, \ldots, x_n]$ with the abstract polynomial ring $\mathbb{F}[X_1, \ldots, X_n]$, we can regard $(*)$ as giving an identity in $\mathbb{F}[X_1, \ldots, X_n, T_1, \ldots, T_n, Z]$. Each of the polynomials appearing in $(*)$ belongs to a subring of $\mathbb{F}[X_1, \ldots, X_n, T_1, \ldots, T_n, Z]$, namely

$$\alpha, \alpha_j \in \mathbb{F}[X_1, \ldots, X_n]$$
$$f \in \mathbb{F}[X_1, \ldots, X_n, Z]$$
$$f_j \in \mathbb{F}[X_1, \ldots, X_n, T_i]$$
$$g \in \mathbb{F}[T_1, \ldots, T_n, Z].$$

We use "$\widehat{\ }$" to denote the substitution process $X_i = x_i$, $T_j = t_j$ and $Z = z$. In particular, we have

$$(**) \qquad \widehat{f} = \widehat{f_j} = \widehat{g} = 0.$$

Also, the defining equations for $\frac{\partial z}{\partial x_i}, \frac{\partial z}{\partial t_j}, \frac{\partial t_j}{\partial x_i}$ can be written

$$\widehat{\frac{\partial f}{\partial Z}} \frac{\partial z}{\partial x_i} = -\widehat{\frac{\partial f}{\partial X_i}} \tag{6}$$

$$\widehat{\frac{\partial g}{\partial Z}} \frac{\partial z}{\partial t_j} = -\widehat{\frac{\partial g}{\partial T_j}} \tag{7}$$

$$\widehat{\frac{\partial f_j}{\partial Z}} \frac{\partial t_j}{\partial x_i} = -\widehat{\frac{\partial f_j}{\partial X_i}}. \tag{8}$$

If we now formally differentiate $(*)$ with respect to each of $\{X_1, \ldots, X_n, T_1, \ldots, T_n, Z\}$ and then substitute $X_i = x_i$, $T_j = t_j$ and $Z = z$ we obtain, using $(**)$, the following identities:

$$\widehat{\frac{\partial g}{\partial T_j}} \widehat{h} = \widehat{a_j} \widehat{\frac{\partial f_j}{\partial T_i}} \tag{9}$$

$$0 = \widehat{a} \widehat{\frac{\partial f_j}{\partial X_i}} + \sum_j \widehat{a_j} \widehat{\frac{\partial f_j}{\partial X_i}} \tag{10}$$

$$\widehat{\frac{\partial f}{\partial Z}} \widehat{h} = \widehat{a} \widehat{\frac{\partial g}{\partial Z}}. \tag{11}$$

These identities can be used to derive the desired chain rule formula because we have the following series of equalities

$$\begin{aligned}
\frac{\partial z}{\partial x_i} &= \left(\widehat{a} \widehat{\frac{\partial f}{\partial X_i}} \right) \Big/ \left(\widehat{a} \widehat{\frac{\partial f}{\partial Z}} \right) \quad \text{(by (6))} \\
&= -\sum_j \left(\widehat{a_j} \widehat{\frac{\partial f_j}{\partial X_i}} \right) \Big/ \left(\widehat{h} \widehat{\frac{\partial g}{\partial Z}} \right) \quad \text{(by (10) and (11))} \\
&= \sum_j \left(\widehat{h} \widehat{\frac{\partial g}{\partial T_j}} \widehat{\frac{\partial f_j}{\partial X_i}} \right) \Big/ \left(\widehat{h} \widehat{\frac{\partial g}{\partial Z}} \widehat{\frac{\partial f_j}{\partial T_i}} \right) \quad \text{(by (9))} \\
&= \sum_j \frac{\partial z}{\partial t_j} \frac{\partial t_j}{\partial x_i} \quad \text{(by (7) and (8))}.
\end{aligned}$$

22 The extended ring of invariants

The ordinary ring of invariants $S(V)^G$ can be extended by introducing an exterior algebra factor. Solomon [1] studied this extended ring of invariants $[S(V) \otimes E(V)]^G$ in the case of pseudo-reflection groups. In this chapter, we describe his results. Solomon's theorem has important applications. It will be used in Chapter 24 to study the occurrence of exterior power representations in the covariant algebra $S(V)/I$. And it will be used in Chapter 32 to study the eigenspaces of elements of pseudo-reflection groups.

In §22-1, we introduce and discuss $E(V)$, the exterior algebra of a vector space V. In §22-2, we study a differential map $d\colon S(V) \otimes E(V) \to S(V) \otimes E(V)$. In §22-3, we study the extended ring of invariants $[S(V)\otimes E(V)]^G$, where $G \subset \mathrm{GL}(V)$ is a pseudo-reflection group. We shall generalize the fact that $S(V)^G$ is a polynomial algebra. In §22-4, we study the Poincaré series of $[S(V) \otimes E(V)]^G$ and extend Molien's theorem from $S(V)^G$ to that case.

22-1 Exterior algebras

Let V be a finite dimensional vector space over the field $\mathbb{F}$. The symmetric algebra $S(V)$ was defined in §16-1. The exterior algebra $E(V)$ is defined in an analogous manner. Let

$$E(V) = T(V)/I,$$

where $T(V)$ is the tensor algebra and

$$I = \text{the graded two-sided ideal generated by } \{x^2 \mid x \in V\}.$$

Then $E(V)$ is a graded, associative, anticommutative algebra. By *anticommutative* we mean that

$$xy = (-1)^{ij} yx$$

if $x \in E_i(V)$ and $y \in E_j(V)$. This anticommutativity property follows from the identities

$$0 = (x + y)^2 = x^2 + xy + yx + y^2 = xy + yx$$

for all $x, y \in V = E_1(V)$.

Notation: We find it convenient to introduce differential form notation. For any $x \in V$, we use the symbol dx to denote its image in $E_1(V) = V$. We use the symbol $x \wedge y$ to denote the product of x and y in $E(V)$.

The grading $T(V) = \bigoplus_{j=0}^{\infty} V^{\otimes j}$ induces the grading on $E(V)$. The graded algebra $E(V)$ is generated by $E_1(V) = V$. If $\{t_1, \dots, t_n\}$ is a basis of V, we write

$$E(V) = E(dt_1, \dots, dt_n).$$

The graded algebra $E(V)$ can be decomposed

$$E(V) = \bigoplus_{k=0}^{n} E_k(V),$$

where, for each $0 \leq k \leq n$, the set

$$\{dt_{i_1} \wedge \cdots \wedge dt_{i_k} \mid i_1 < \cdots < i_k\}$$

is an $\mathbb{F}$ basis of $E_k(V)$.

There are two ways to extend the above discussion. Each was already discussed in Chapter 16 for the case $S(V)$. First of all, we can extend the exterior algebra notation $E(V) = E(dt_1, \ldots, dt_n)$ to include the case where V is a graded vector space and $\{t_1, \ldots, t_n\}$ is a homogeneous basis of V, with the elements $\{t_1, \ldots, t_n\}$ allowed to have arbitrary degree. Secondly, we can also consider the exterior algebra $E(V^*)$ on the dual of V. Just as $S(V^*)$ can be interpreted as polynomial functions on V, so $E(V^*)$ can be interpreted as alternating functions on V.

22-2 The differential d: $S(V) \otimes E(V) \to S(V) \otimes E(V)$

The map d: $V \to E(V)$ extends to a differential map

$$d\colon S(V) \otimes E(V) \to S(V) \otimes E(V)$$

by the rule that

$$d(x) = 0 \quad \text{for all } x \in E(V)$$
$$d(xy) = d(x)y + xd(y) \quad \text{for all } x, y \in S(V) \otimes E(V).$$

The map d is compatible with the gradings of both $S(V)$ and $E(V)$ in that it restricts to give maps

$$d\colon S_i(V) \otimes E_j(V) \to S_{i-1}(V) \otimes E_{j+1}(V).$$

Given any $x \in S(V) \otimes E(V)$, we use dx to denote its image under the map d. We shall be using the notation $dx \wedge dy$ to denote the multiplication of the elements dx and dy in $S(V) \otimes E(V)$.

The action of G on V also induces an action on $E(V)$. The process is similar to that described in §21-1 for inducing an action on $S(V)$. Thus we also have an action of G on $S(V) \otimes E(V)$. We use this action throughout this chapter. In particular, we can consider the invariants $[S(V) \otimes E(V)]^G$. The goal is to show that the elements $\{dx_i\}$ generate an exterior subalgebra

$$E(dx_1, \ldots, dx_n) \subset S(V) \otimes E(V).$$

The Jacobian J from Chapter 21 will play a part in our argument. It arises naturally in the context of the differential map d. Let $\{t_1, \ldots, t_n\}$ be a basis of V. If $G \subset \mathrm{GL}(V)$ *is a finite nonmodular pseudo-reflection group*, then we can write

$$S(V) = \mathbb{F}[t_1, \ldots, t_n]$$
$$S(V)^G = \mathbb{F}[x_1, \ldots, x_n].$$

The elements $\{dx_i\}$ can be expanded in $S(V) \otimes E(V)$ using the standard partial derivative formula

$$dx_i = \sum_j \frac{\partial x_i}{\partial t_j} dt_j.$$

It follows from the anticommutative property of the elements $\{dt_j\}$ that the Jacobian $J = \det[\frac{\partial x_i}{\partial t_j}]$ satisfies the following identity in $S(V) \otimes E(V)$.

Lemma A $dx_1 \wedge \cdots \wedge dx_n = J(dt_1 \wedge \cdots \wedge dt_n)$.

Remark: It was shown by an indirect argument in §21-2 that the Jacobian is skew. The above J formula provides a direct and natural way of demonstrating that J is skew. First of all, given $\varphi \in G$, if we apply φ to the identity of Lemma A, we obtain

$$\varphi \cdot (dx_1 \wedge \cdots \wedge dx_n) = (\varphi \cdot J)\varphi \cdot (dt_1 \wedge \cdots \wedge dt_n).$$

Since each $dx_i \in [S(V) \otimes E(V)]^G$ (this is discussed in more detail in §22-3), we have the identity

$$\varphi \cdot (dx_1 \wedge \cdots \wedge dx_n) = dx_1 \wedge \cdots \wedge dx_n.$$

Lastly, we have the standard formula from multilinear algebra for defining the determinant:

$$\varphi \cdot (dt_1 \wedge \cdots \wedge dt_n) = \det(\varphi) dt_1 \wedge \cdots \wedge dt_n.$$

By comparing these three equations, we obtain

$$\varphi \cdot J = \det(\varphi)^{-1} J$$

and, so, J is skew.

We now turn to showing that the elements $\{dx_i\}$ generate an exterior subalgebra

$$E(dx_1, \ldots, dx_n) \subset S(V) \otimes E(V).$$

First of all, $\{dx_i\}$ satisfy:

Lemma B $dx_i \wedge dx_j = -dx_j \wedge dx_i$.

Proof As already observed, we can write each dx_i, as an element of $S(V) \otimes E(V)$, in the form

$$dx_i = \sum_j \frac{\partial x_i}{\partial t_j} dt_j.$$

The presence of the factors $\{dt_j\}$ force $\{dx_i\}$ to be anticommutative. ■

Next, for each $I \subset \{1, \ldots, n\}$, let

$$dx_I = dx_{i_1} \wedge \cdots \wedge dx_{i_k},$$

where $I = \{i_1 < \cdots < i_k\}$.

Lemma C *The elements $\{dx_I\}$ are linearly independent.*

Proof Given any relation

$$\sum_I c_I dx_I = 0,$$

where $c_I \in \mathbb{F}$, fix $J \subset \{1, \ldots, n\}$ and multiply both sides by dx_K, where $K =$ the complement of J in $\{1, \ldots, n\}$. Since $dx_I \wedge dx_K = 0$ if $I \cap K \neq \varnothing$, we obtain

$$c_J(dx_1 \wedge \cdots \wedge dx_n) = 0.$$

However, by Lemma A and Proposition 21-1B, we also have

$$dx_1 \wedge \cdots \wedge dx_n \neq 0.$$

Hence the only possibility is $c_J = 0$. ■

22-3 Invariants of $S(V) \otimes E(V)$

In this section, following arguments of Solomon, we shall calculate the invariants of $S(V) \otimes E(V)$ for pseudo-reflection groups $G \subset \mathrm{GL}(V)$. The differential map $d\colon S(V) \otimes E(V) \to S(V) \otimes E(V)$ defined in §22-2 commutes with the action of G and, so, it defines a map

$$d\colon [S(V) \otimes E(V)]^G \to [S(V) \otimes E(V)]^G.$$

By §23-1, we can write

$$S(V)^G = \mathbb{F}[x_1, \ldots, x_n].$$

We have $dx_i \in [S(V) \otimes E(V)]^G$. It was shown in §22-2 that the elements $\{dx_i\}$ generate an exterior subalgebra

$$E(dx_1, \ldots, dx_n) \subset [S(V) \otimes E(V)]^G.$$

The rest of this section is devoted to proving:

***Theorem* (Solomon)** *Let $G \subset \mathrm{GL}(V)$ be a finite nonmodular pseudo-reflection group. Then*

$$[S(V) \otimes E(V)]^G = \mathbb{F}[x_1, \ldots, x_n] \otimes E(dx_1, \ldots, dx_n).$$

If $\{t_1, \ldots, t_n\}$ is an $\mathbb{F}$ basis of V, we write

$$S = S(V) = \mathbb{F}[t_1, \ldots, t_n]$$

$$E = E(V) = E(dt_1, \ldots, dt_n).$$

Also, as before, for each $I \subset \{1, \ldots, n\}$, we let

$$dt_I = dt_{i_1} \wedge \cdots \wedge dt_{i_k} \quad \text{and} \quad dx_I = dx_{i_1} \wedge \cdots \wedge dx_{i_k},$$

where $I = \{i_1 < \cdots < i_k\}$.

We shall prove the above theorem by a series of lemmas. Let $F(S)$ be the quotient field of S. The action of G on S extends to an action of G on $F(S)$. Namely,

$$\varphi \cdot (x/y) = (\varphi \cdot x)/(\varphi \cdot y)$$

for any $x, y \in S$. We first show:

Lemma A $F(S) \otimes E = F(S) \otimes E(dx_1, \ldots, dx_n)$.

Proof Treat $F(S) \otimes E$ as a vector space over $F(S)$. We want to show that the set $\{dx_I \mid I \subset \{1, \ldots, n\}\}$ is an $F(S)$ basis of $F(S) \otimes E$. First of all, as in Lemma 22-2C, the set $\{dx_I\}$ is linearly independent over $F(S)$. It now follows from a counting argument that the monomials $\{dx_I\}$ are an $F(S)$ basis of $F(S) \otimes E$ because, since $\{dt_I\}$ is an $F(S)$ basis of $F(S) \otimes E$, any 2^n linearly independent elements are also a basis. ■

Lemma B $\left(F(S) \otimes E\right)^G = F(S)^G \otimes E(dx_1, \ldots, dx_n)$.

Proof Treat $\left(F(S) \otimes G\right)^G$ as a vector space over the field $F(S)^G$. We want to show that the monomials $\{dx_I\}$ are a basis of $\left(F(S) \otimes E\right)^G$. By Lemma A, we need only show $\{dx_I\}$ span $\left(F(S) \otimes E\right)^G$. Given $y \in \left(F(S) \otimes E\right)^G \subset F(S) \otimes E$, we know from Lemma A that

$$y = \sum_I c_I dx_I,$$

where $c_I \in F(S)$. If we apply the averaging operator $\mathrm{Av} = \frac{1}{|G|} \sum_{\varphi \in G} \varphi$ defined in §14-3, then we obtain from Lemmas A and B of §14-3 that

$$y = \sum_I \mathrm{Av}(c_I) dx_I.$$

So now the coefficients $\mathrm{Av}(c_I)$ belong to $F(S)^G$. ■

Lastly, we prove the theorem.

Proof of Solomon's Theorem We want

$$(S \otimes E)^G = S^G \otimes E(dx_1, \ldots, dx_n).$$

By Lemma B, we need only show that the monomials $\{dx_I\}$ span the S^G module $(S \otimes E)^G$. Given $y \in (S \otimes E)^G$, then, by Lemma B, we can expand

$$y = \sum_I c_I dx_I,$$

where $c_I \in F(S)^G$. We want to show that $c_I \in S^G$. It suffices to show that $c_I \in S$. If we multiply both sides of this identity by dx_K, where $K =$ the complement of I in $\{1, \ldots, n\}$, then

$$dx_K y = c_I$$

$$c_I(dx_1 \wedge \cdots \wedge dx_n) = c_I J(dt_1 \wedge \cdots \wedge dt_n).$$

Since the LHS belongs to $(S \otimes E)^G$, it follows that the RHS belongs to $(S \otimes E)^G$ as well. In particular, the RHS belongs to $S \otimes E$. So

$$c_I J \in S.$$

The factorization $c_I J$ is known to hold in $F(S)$, but it is not clear whether it holds in S. We need to show that

$$c_I \in S,$$

which we shall now do. Since $\varphi \cdot c_I = c_I$ and $\varphi \cdot J = (\det \varphi)^{-1} J$, we know that $c_I J$ is a skew invariant of S. By Proposition 20-2B and Proposition 21-1B, $c_I J$ is divisible by J in S. In other words, $c_I \in S$. ■

22-4 The Poincaré series of $[S(V) \otimes E(V)]^G$

As in the previous section, let $S = S(V)$ and $E = E(V)$. We can consider $S \otimes E$ as being bigraded via the decomposition

$$S \otimes E = \bigoplus_{i,j} S_i \otimes E_j.$$

So $(S \otimes E)^G \subset S \otimes E$ inherits a bigrading. The Poincaré series of $(S \otimes E)^G$ is a power series in two variables

$$P = \sum_{i,j} a_{ij} X^i Y^j,$$

where

$$a_{ij} = \dim_{\mathbb{F}} S_i \otimes E_j.$$

We now give an explicit description of this Poincaré series. This description will be very useful in subsequent chapters. Indeed, in terms of future applications, it is the most important result of this chapter.

Proposition

$$P = \frac{\prod_{i=1}^n (1 + YX^{d_i - 1})}{\prod_{i=1}^n (1 - X^{d_i})} = \frac{1}{|G|} \sum_{\varphi \in G} \frac{\det(1 + Y\varphi)}{\det(1 - X\varphi)}.$$

Proof It follows from Theorem 22-3 that

$$(*) \qquad P = \prod_{i=1}^{n} (1 + YX^{d_i - 1}) / \prod_{i=1}^{n} (1 - X^{d_i}).$$

On the other hand, a simple adaptation of the argument in Chapter 17 yields the following generalization of Molien's Theorem

$$(**) \qquad P = \frac{1}{|G|} \sum_{\varphi \in G} \frac{\det(1 + Y\varphi)}{\det(1 - X\varphi)}.$$

In particular, in analogue to Proposition A of §17-2, we have the identity

$$\det(1 + \varphi t) = \sum \operatorname{tr}(\varphi_i) t^i,$$

where $\varphi_i \colon E_i \to E_i$ is the map induced by φ. This identity, along with Propositions A and B of §17-2, implies $(**)$. By combining $(*)$ and $(**)$, we have the identity stated in the proposition. ■

VII Rings of covariants

We have been studying the strong interaction between a group $G \subset \mathrm{GL}(V)$ and its ring of invariants $S(V)^G$. In the next few chapters, we turn instead to the ring of covariants. These chapters are concerned with the ways in which the structure of a pseudo-reflection group is mirrored in the structure of its covariant ring. The themes pursued are somewhat diverse, but are all closely related to this central question. In Chapter 23, we study the Poincaré series for the ring of covariants in the case of a Euclidean reflection group. In Chapter 24, we study the representation theory of pseudo-reflection groups. The action of G on the covariants plays an important role in this study. In the nonmodular case, this action gives the regular representation. In Chapters 25 and 26, we study the harmonic polynomials of a group $G \subset \mathrm{GL}(V)$ and demonstrate that, in the case where the ground field is of characteristic zero, G being a pseudo-reflection group can be characterized in terms of the harmonics. We also use this characterization of pseudo-reflection groups to prove that every isotropy subgroup of a pseudo-reflection group is a pseudo-reflection group. This property of isotropy subgroups will play a significant role in Chapter 34 when the regular elements of pseudo-reflection groups are studied.

23 Poincaré series for the ring of covariants

The main goal of this chapter is to study the Poincaré series of Euclidean reflection groups. As an application of these results, we shall demonstrate a very explicit, and effective, method of calculating the degrees and exponents of a Weyl group from its underlying crystallographic root system. This chapter relies heavily on the results of Demazure [1].

23-1 Poincaré series

Let V be a finite dimensional vector space over $\mathbb{F}$ and let $G \subset \mathrm{GL}(V)$ *be a finite nonmodular pseudo-reflection group.* Let

$$S = S(V), \qquad \text{the symmetric algebra of } V$$

$$I = \text{the graded ideal of } S \text{ generated by the homogeneous elements from } S^G \text{ of positive degree.}$$

In the next four chapters, we shall study the ring of covariants

$$S_G = S/I.$$

In this chapter, we focus on Poincaré series, i.e., on the structure of S_G as a graded $\mathbb{F}$ vector space. In later chapters, we shall focus on other aspects of S_G. In Chapter 24, we shall study its structure as a G module, and in Chapters 25 and 26 we shall study the associated module of harmonics $H \subset S$.

We began the study of the Poincaré series of S_G in Chapter 20. Let $n = \dim_{\mathbb{F}} V$ and let $\{d_1, \dots, d_n\}$ be the degrees of G. It was shown in §20-3 that:

Theorem A *Let $G \subset \mathrm{GL}(V)$ be a finite nonmodular pseudo-reflection group. Then*

$$P_t(S_G) = \prod_{i=1}^{n} \frac{1 - t^{d_i}}{1 - t} = \prod_{i=1}^{n} [1 + t + \cdots + t^{d_i - 1}].$$

In particular, letting $t = 1$ and using the fact that $|G| = \prod_{i=1}^{n} d_i$, we obtain:

Corollary $\dim_{\mathbb{F}} S_G = |G|$.

It follows from Theorem A that the degrees $\{d_1, \dots, d_n\}$ of G are related to the Poincaré series of S_G. In the rest of this chapter, we develop an alternative formula for $P_t(S_G)$ in the case of Euclidean reflection groups. When we combine these formulas with the one above from Theorem A, we shall have a highly effective method of calculating $\{d_1, \dots, d_n\}$.

The chapter will be devoted to proving the following theorem.

Theorem B *Let $W \subset \mathrm{GL}(\mathbb{E})$ be a finite Euclidean reflection group. Then*

$$P_t(S_W) = \sum_{\varphi \in W} t^{\ell(\varphi)}.$$

In the above equation, ℓ denotes length in W. To define length, we have to choose a root system $\Delta \subset \mathbb{E}$ for W, and then a fundamental system Σ of Δ (see §4-2). As already observed in §13-1, the polynomial $\sum_{\varphi\in W} t^{\ell(\varphi)}$ is independent of these choices.

Before providing the proof of Theorem B, we shall first demonstrate its importance. We shall combine Theorems A and B from §23-2 to obtain a formula for calculating degrees, and then apply the formula to the case of Weyl groups.

In all that follows, we shall let $\Delta \subset \mathbb{E}$ be a root system with associated reflection group $W = W(\Delta)$. We shall let $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$ be a fundamental system of Δ and $\{s_1, \ldots, s_\ell\}$ be the corresponding fundamental reflections in W.

23-2 The exponents of Weyl groups

In this section, we specialize to the case of crystallographic reflection groups for the sake of a particular application of Theorem 23-1B. It will be demonstrated that we can combine Theorem 23-1B with other results to obtain an effective method of calculating the degrees and exponents of crystallographic reflection groups. It will be shown that, for a crystallographic root system Δ, the degrees and exponents of $W(\Delta)$ are directly calculable from Δ.

Let $\Delta \subset \mathbb{E}$ be a crystallographic root system and let $W = W(\Delta)$ be its associated Weyl group. In Chapter 13, we proved that, for any crystallographic root system, we have the identity

$$\sum_{\varphi\in W} t^{\ell(\varphi)} = \prod_{\alpha\in\Delta^+} \frac{t^{h(\alpha)+1} - 1}{t^{h(\alpha)} - 1}.$$

Here Δ^+ are the positive roots, ℓ denotes length in W, and h denotes height in Δ, all defined with respect to some specific fundamental system in Δ. The polynomials on both sides of the identity are independent of the particular choice of the fundamental system.

When we combine the above identity with Theorems A and B from §23-1, we have the identity

$$\prod_{i=1}^{n} \frac{t^{d_i} - 1}{t - 1} = \prod_{\alpha\in\Delta^+} \frac{t^{h(\alpha)+1} - 1}{t^{h(\alpha)} - 1}.$$

This identity provides a way of calculating the degrees $\{d_1, \ldots, d_\ell\}$, the exponents $\{m_1, \ldots, m_\ell\}$ of W, or both. The method was originally observed empirically by Shapiro, and thereafter justified theoretically by Kostant [1] using Lie theoretic methods. The more elementary approach of this chapter is due to MacDonald [2].

The main result will be stated in terms of *dual partitions*. Duality between partitions is most easily envisaged with the help of diagrams. For example, the diagram

```
* * * * * * *
* * *
*
```

illustrates that $\{7,3,1\}$ and $\{3,2,2,1,1,1,1\}$ are dual partitions of 11.

Let

$$n_k = \text{the number of positive roots of height k.}$$

We know that both $\{n_1, n_2, \dots\}$ and $\{m_1, m_2, \dots\}$ are partitions of N (= the number of positive roots). For, by definition, $n_1 + n_2 + \cdots = N$ whereas, by Corollary 18-1, $m_1 + m_2 + \cdots = N$. It can be deduced from the above polynomial identity that:

Theorem *$\{n_1, n_2, \dots\}$ and $\{m_1, m_2, \dots\}$ are dual partitions of N.*

This theorem provides a direct link between the exponents of Weyl groups and their root systems. The same is therefore true for degrees (recall that $d_i = m_i + 1$).

Example: As an illustration of the use of the theorem, consider the root system $\Delta = B_3$ (see §3-3). If we arrange the positive roots by height, then we have a diagram of the form

$$\begin{array}{ccc} * & * & * \\ * & * & \\ * & * & \\ * & & \\ * & & \end{array}$$

So $\{n_1, n_2, n_3, n_4, n_5\} = \{3,2,2,1,1\}$. It follows that $\{m_1, m_2, m_3\} = \{1,3,5\}$. Hence, we have determined the degrees $\{d_1, d_2, d_3\} = \{2,4,6\}$ of $W(B_3)$ from its root system B_3.

To prove the theorem, it suffices to prove:

Proposition

(i) $n_1 \geq n_2 \geq n_3 \geq \cdots$;
(ii) $n_k - n_{k+1}$ = *the number of times that* $k+1$ *occurs in the degrees* $\{d_1, \dots, d_\ell\}$.

This proposition asserts that $n_k - n_{k+1}$ = the number of times that k occurs in the exponents $\{m_1, \dots, m_\ell\}$. As the above diagrams illustrate, this relation is equivalent to the theorem.

The proof of the proposition is based on the unique factorization of polynomials in $\mathbb{Z}[t]$ into irreducible factors. The polynomials $t^k - 1$ are not irreducible but, nevertheless, we can show that:

Lemma *A decomposition in $\mathbb{Z}[t]$ of the form $f(t) = (t-1)^{e_1}(t^2-1)^{e_2}\cdots(t^k-1)^{e_k}$ is unique.*

Proof This is based on the fact that $t^k - 1$ has an unique *cyclotomic decomposition*

$$(*) \qquad t^k - 1 = \prod_{s|k} \Psi_s(t)$$

into irreducible factors, where $\Psi_s(t)$ is the s-th cyclotomic polynomial. The cyclotomic polynomials are irreducible in $\mathbb{Z}[t]$. Since $\mathbb{Z}[t]$ is a unique factorization domain, this cyclotomic decomposition is unique. We observe that

$$(**) \qquad \Psi_k(t) \text{ appears in } t^k - 1 \text{ but not in } t^i - 1 \text{ for } i < k.$$

Given a *power decomposition* $f(t) = (t-1)^{e_1}(t^2-1)^{e_2}\cdots(t^k-1)^{e_k}$, we can further decompose $f(t)$ into copies of the various $\Psi_s(t)$.

We now can make an inductive argument showing that any two power decompositions of $f(t)$ must have the same factors with the same multiplicity for each factor $t^k - 1$. We proceed by downward induction on degree, i.e., on k. If $t^k - 1$ is the highest-degree factor appearing in a power decomposition of $f(t)$, then, because of $(**)$, the number of copies of $t^k - 1$ in $(*)$ agrees with the number of copies of $\Psi_s(t)$ appearing in the (unique!) cyclotomic decomposition of $f(t)$. So any two power decompositions of $f(t)$ must have the same highest-degree factor with the same multiplicity. Cancelling these terms, we continue the argument with the next highest-degree terms. ∎

Proof of Proposition It is now an easy argument to establish the above proposition. Clearly, (ii) forces (i). To prove (ii), we take the previous identity

$$\prod_{i=1}^{n} \frac{t^{d_i} - 1}{t - 1} = \prod_{\alpha\in\Delta^+} \frac{t^{h(\alpha)+1} - 1}{t^{h(\alpha)} - 1}$$

and, by cross-multiplication, obtain the identity

$$\left[\prod_{\alpha\in\Delta^+} (t^{h(\alpha)} - 1)\right]\left[\prod_{i=1}^{n}(t^{d_i} - 1)\right] = (t-1)^n \prod_{\alpha\in\Delta^+} (t^{h(\alpha)+1} - 1).$$

By the above lemma, the same terms must be present on each side.

23-3 The Δ operations

To prove the identity $P_t(S_W) = \sum_{\varphi\in W} t^{\ell(\varphi)}$, we shall use the Δ operations defined in §18-2. Recall that, for any reflection $s \in W$, we can define the operation

$$\Delta\colon S \to S$$

by the rule

$$s \cdot x = x + \Delta(x)\alpha.$$

The Δ operations are *twisted derivations* satisfying

$$\Delta(xy) = \Delta(x)y + (s\cdot x)\Delta(y)$$

for any $x, y \in S$. They annihilate S^W, and so induce maps $\Delta\colon I \to I$ (by the rule $\Delta(xy) = x\Delta(y)$ for $x \in S^W$ and $y \in S$). Thus we also have induced maps

$$\Delta\colon S_W \to S_W.$$

Let $\{s_1, \dots, s_\ell\}$ be the fundamental reflections of W and let $\{\Delta_1, \dots, \Delta_\ell\}$ be their associated Δ operations.

Lemma *If $0 \neq x \in S_W$ has degree k, then there exists $i_1, \dots, i_k$ chosen from $\{1, \dots, \ell\}$ (with repetitions allowed) such that $\Delta_{i_1} \cdots \Delta_{i_k}(x) \neq 0$ in $(S_W)_o = \mathbb{F}$.*

Proof The proof of Lemma 18-2C can be easily modified to show that, if $0 \neq y \in S_W$ has degree > 0, then $\Delta_i(y) \neq 0$ for some $1 \leq i \leq \ell$. The lemma follows from repeated applications of this fact. ■

The proof of the identity $P_t(S_W) = \sum_{\varphi \in W} t^{\ell(\varphi)}$ is a refinement of the above lemma. For any composite $\Delta_{i_1} \cdots \Delta_{i_k}$, we have the associated operation $s_{i_1} \cdots s_{i_k} \in W$. Recall that $s_{i_1} \cdots s_{i_k}$ is called a *reduced expression* if $\ell(s_{i_1} \cdots s_{i_k}) = k$. The rest of the chapter will be devoted to proving:

Proposition *If $s_{i_1} \cdots s_{i_k}$ and $s_{j_1} \cdots s_{j_k}$ are two reduced expressions of the same $\varphi \in W$, then $\Delta_{i_1} \cdots \Delta_{i_k} = \Delta_{j_1} \cdots \Delta_{j_k}$.*

This result holds in S and, hence, in S_W. It suffices to prove the identity $P_t(S_w) = \sum_{\varphi \in W} t^{\ell(\varphi)}$. First of all, we observe a consequence of the proposition.

Corollary *If $\ell(s_{i_1} \cdots s_{i_k}) < k$ then $\Delta_{i_1} \cdots \Delta_{i_k} = 0$.*

Proof It follows from the Matsumoto Exchange Property (see Theorem 4-4B) that, for some $1 \leq a \leq b < k$,

$$s_{i_a} \cdots s_{i_b} = s_{i_{a+1}} \cdots s_{i_{b+1}}.$$

Choose a and b such that $b - a$ is minimal. Then $s_{i_a} \cdots s_{i_b}$ and $s_{i_{a+1}} \cdots s_{i_{b+1}}$ are reduced expressions. Otherwise, we could apply the Matsumoto Exchange Property to the expressions $s_{i_a} \cdots s_{i_b}$ or $s_{i_{a+1}} \cdots s_{j_{b+1}}$ and deduce that $b - a$ is not minimal. The proposition implies that

$$\Delta_{i_a} \cdots \Delta_{i_b} = \Delta_{i_{a+1}} \cdots \Delta_{i_{b+1}}.$$

It follows that

$$\Delta_{i_1} \cdots \Delta_{i_k} = \Delta_{i_1} \cdots \hat{\Delta}_{i_a} \Delta_{i_{a+1}} \cdots \Delta_{i_{b+1}} \Delta_{i_{b+1}} \cdots \Delta_{i_k} = 0.$$

where "$\wedge$" denotes elimination. Regarding the last equality, for any $\alpha \in \Delta$, $(s_\alpha)^2 = 1$ forces $(\Delta_\alpha)^2 = 0$. Consequently, $(\Delta_{i_{b+1}})^2 = 0$. ■

Now let

$$r_k = \text{the rank of } S_W \text{ in dimension } k$$
$$\ell_k = \text{the number of elements in } W \text{ of length } k.$$

The above desired Poincaré series identity is equivalent to asserting that $r_k = \ell_k$ for all k. By combining the above lemma, proposition and corollary we conclude that

$$r_k \leq \ell_k \quad \text{for all } k.$$

On the other hand, the identity $\dim_{\mathbb{F}} S_W = |W|$ tells us that

$$\sum r_i = \sum \ell_i.$$

These two relations force $r_k = \ell_k$. So we are left with proving the above proposition.

23-4 The element ω_o

The proof of Proposition 23-3 proceeds by first establishing the proposition for a canonical element $\omega_o \in W$. The fundamental system $\Sigma \subset \Delta$ determines a decomposition

$$\Delta = \Delta^+ \coprod \Delta^-$$

of Δ into positive and negative roots. In §27-1, it will be explained how to choose a unique involution $\omega_o \in W$ with the property that it converts every positive root into a negative root, i.e.,

$$\omega_o \Delta^+ = \Delta^-.$$

Since the length $\ell(\varphi)$ (with respect to Σ) of each $\varphi \in W$ can be determined by counting the number of positive roots of Δ transformed by φ into negative roots, we have

$$\ell(\omega_o) = N \quad \text{where } N = |\Delta^+|.$$

As will be observed in §27-1, ω_o is the "longest word", namely the unique element in W of maximal length ($= N$) with respect to Σ.

In this section, we show that Proposition 23-3 holds for all the reduced expressions of ω_o, i.e., for every decomposition $\omega_o = s_{\alpha_1} \cdots s_{\alpha_N}$ of ω_o using N fundamental reflections (see §4). Let

$$\mathcal{S}k \colon S \to S$$

be the skew operator defined in §20-1, and let $\Omega = \prod_{\alpha > 0} \alpha$ be the skew-invariant element of S defined in §20-2. In this section we shall prove:

Proposition *If $\omega_o = s_{i_1} \cdots s_{i_N}$ then, for all $x \in S$,*

$$\Delta_{i_1} \cdots \Delta_{i_N}(x) = \mathcal{S}k(x)/\Omega.$$

Observe that $\mathcal{S}k(x)$ is a skew invariant and, so, divisible by Ω. Hence, $\mathcal{S}k(x)/\Omega \in S$. The proposition shows that the action of $\Delta_{i_1} \cdots \Delta_{i_N}$ is the same for each reduced expression $s_{i_1} \cdots s_{i_N}$ of ω_o.

We shall prove the above proposition in two steps.

(I) $\Omega\Delta_{i_1} \cdots \Delta_{i_N} = \lambda \mathcal{S}k$ for some $\lambda \in \mathbb{F}$;
(II) $\lambda = 1$.

Step I First of all, we consider the action of $\Omega\Delta_{i_1} \cdots \Delta_{i_N}$ and $\mathcal{S}k$ on Ω. We have $\mathcal{S}k(\Omega) = \Omega$ while $\Delta_{i_1} \cdots \Delta_{i_N}(\Omega) = \lambda \in S_o = \mathbb{F}$. So $\Omega\Delta_{i_1} \cdots \Delta_{i_N}(\Omega) = \lambda\Omega$. Hence,

$$\Omega\Delta_{i_1} \cdots \Delta_{i_N}(\Omega) = \lambda \mathcal{S}k(\Omega).$$

We now use this equality to force the equality $\Omega\Delta_{i_1} \cdots \Delta_{i_N}(x) = \lambda \mathcal{S}k(x)$ for all $x \in S$.

We know, from §18-3, that S is a free S^W module. Moreover, both $\mathcal{S}k\colon S \to S$ and $\Delta_{i_1} \cdots \Delta_{i_N}\colon S \to S$ are S^W module maps. So it suffices to show that $\Omega\Delta_{i_1} \cdots \Delta_{i_N}$ and $\mathcal{S}k$ differ by $\lambda \in \mathbb{F}$ when they act on a set of S^W generators of S.

First of all, in degrees $\geq N$, the only S^W generator that need be considered is Ω because a set of S^W generators of S projects to an $\mathbb{F}$ basis of $S_W = S/I$, and it was established in §20-3 that

$$S_W = \begin{cases} 0 & \text{if degree} > N \\ \mathbb{F}\Omega & \text{if degree} = N. \end{cases}$$

Secondly, in degrees $\leq N$, the only S^W generator that need be considered is also Ω because, since $\mathcal{S}k$ takes values in the skew invariants of S and since every skew invariant is divisible by Ω, it follows that $\mathcal{S}k = 0$ in degree $< N$. Moreover, since $\Delta_{i_1} \cdots \Delta_{i_N}$ lowers degree by N, we also have $\Delta_{i_1} \cdots \Delta_{i_N} = 0$ in degree $< N$.

We can now finish the proof that $\Omega\Delta_{i_1} \cdots \Delta_{i_N} = \lambda \mathcal{S}k$. By the above restrictions, $\mathcal{S}k$ and $\Delta_{i_1} \cdots \Delta_{i_N}$ are determined by their effect on Ω. Since $\mathcal{S}k(\Omega) = \Omega$ and $\Delta_{i_1} \cdots \Delta_{i_N}(\Omega) = \lambda$, the equality $\Omega\Delta_{i_1} \cdots \Delta_{i_N} = \lambda \mathcal{S}k$ follows.

Step II As in §4-4, for any $\varphi \in W$, let:

Definition: $\Delta(\varphi) = \Delta^+ \cap \varphi^{-1}\Delta^- =$ the positive roots of Δ transformed by φ into negative roots.

The fact that $\lambda = 1$ follows from the next general fact. We need to work in $F(S) =$ the fraction field of S. We use the notation x/y to denote the element xy^{-1} in $F(S)$. The action of W on S extends to an action on $F(S)$ by the rule

$$\varphi \cdot (x/y) = (\varphi \cdot x)/(\varphi \cdot y) \quad \text{for all } x, y \in S \text{ and } \varphi \in W.$$

It follows that the operations $\Delta_\alpha = \alpha^{-1}(1 - s_\alpha)$ also extend to an action on $F(S)$. Working in $F(S)$, we obtain:

Lemma C *If $\varphi = s_{i_1} \cdots s_{i_k}$ is a reduced expression for φ, then*

$$\Big[\prod_{\alpha \in \Delta(\varphi^{-1})} \alpha \Big] \Delta_{i_1} \cdots \Delta_{i_k} = (\det \varphi)\varphi + \sum_{\ell(\phi) < \ell(\varphi)} C_\phi \phi,$$

where $C_\phi \in F(S)$.

We conclude that $\lambda = 1$ by applying this lemma to the element $\omega_0 = s_{i_1} \cdots s_{i_N}$ defined in §23-1. Recall that we have $\omega_o = \omega_o^{-1}$ (i.e., ω_o is an involution) and $\Delta(\omega_o^{-1}) = \Delta(\omega_o) = \Delta^+$. Consequently, $\prod \alpha_{\alpha \in \Delta(\omega_0^{-1})} = \Omega$ and the identity in Lemma C becomes

$$(*) \qquad \Omega \Delta_{i_1} \cdots \Delta_{i_N} = (\det \omega_o)\omega_o + \sum_{\ell(\phi) < \ell(\omega_0)} C_\phi \phi.$$

On the other hand, by Step I

$$(**) \qquad \Omega \Delta_{i_1} \cdots \Delta_{i_N} = \lambda \mathcal{S}k = \lambda(\det \omega_o)\omega_o + \text{other terms.}$$

So $(*)$ and $(**)$ force $\lambda = 1$.

Proof of Lemma C We shall work in $F(S)$. We know from Theorem 4-4D that, if $\varphi = s_{i_1} \cdots s_{i_k}$, then

$$\Delta(\varphi^{-1}) = \{\alpha_{i_1}, s_{i_1} \cdot \alpha_{i_2}, \ldots, (s_{i_1} s_{i_2} \cdots s_{i_{k-1}}) \cdot \alpha_{i_k}\}.$$

On the other hand, the identity $\Delta_\alpha = \alpha^{-1}(1 - s_\alpha)$ tells us that

$$\begin{aligned}
\Delta_{i_1} \cdots \Delta_{i_k} &= \alpha_{i_1}^{-1}(1 - s_{i_1}) \cdots \alpha_{i_k}^{-1}(1 - s_{i_k}) \\
&= [(\alpha_{i_1})(s_{i_1} \cdot \alpha_{i_2}) \cdots (s_{i_1} \cdots s_{i_{k-1}} \cdot \alpha_{i_k})]^{-1}(-1)^k s_{i_1} \cdots s_{i_k} + \sum_{\ell(\phi) < k} C_\phi \phi \\
&= \Big[\prod_{\alpha \in \Delta(\varphi^{-1})} \alpha \Big]^{-1} \det(\varphi)\varphi + \sum_{\ell(\phi) < k} C_\phi \phi.
\end{aligned}$$

This concludes the proof of the lemma. ■

23-5 The proof of Proposition 23-3

In this section we prove Proposition 23-3. We show that $\Delta_{i_1} \cdots \Delta_{i_k} = \Delta_{j_1} \cdots \Delta_{j_k}$ if $s_{i_1} \cdots s_{i_k}$ and $s_{j_1} \cdots s_{j_k}$ are reduced expressions for the same $\varphi \in W$. We begin by considering a special case.

Dihedral Reflection Groups If $W = \langle s_\alpha, s_\beta \mid (s_\alpha)^2 = (s_\beta)^2 = (s_\alpha s_\beta)^m = 1\rangle$, then the only element of W with two distinct reduced expressions is the longest word

$$\omega_o = s_\alpha s_\beta s_\alpha \cdots = s_\beta s_\alpha s_\beta \cdots \quad (m \text{ terms in each expression}).$$

By §23-4, we must have

$$\Delta_\alpha \Delta_\beta \Delta_\alpha \cdots = \Delta_\beta \Delta_\alpha \Delta_\beta \cdots .$$

Before proving the general case, we also want to record a lemma that will play an important role in the argument.

Lemma *If $s_{i_1} \cdots s_{i_k}$ and $s_{j_1} \cdots s_{j_k}$ are reduced expressions for $\varphi \in W$, then $s_{i_1} s_{j_1} s_{j_2} \cdots \hat{s}_{j_q} \cdots s_{j_{k-1}} s_{j_k}$ is also a reduced expression for φ, for some $1 \leq q \leq k$.*

Proof Since

$$s_{i_1} s_{j_1} \cdots s_{j_k} = s_{i_1} s_{i_1} \cdots s_{i_k} = s_{i_2} \cdots s_{i_k},$$

we know $\ell(s_{i_1} s_{j_1} \cdots s_{j_k}) < k+1$. Therefore, by the Matsumoto Cancellation Property (see Theorem 4-4C), we can delete two entries from $s_{i_1} s_{j_1} \cdots s_{j_k}$. The possible deletions are

(i) $s_{i_1} s_{j_1} \cdots \hat{s}_{j_q} \cdots \hat{s}_{j_r} \cdots s_{j_k}$;
(ii) $\hat{s}_{i_1} s_{j_1} \cdots \hat{s}_{j_q} \cdots s_{j_k}$.

Case (i) is impossible because the equality $s_{i_1} s_{j_1} \cdots s_{j_k} = s_{i_1} s_{j_1} \cdots \hat{s}_{j_q} \cdots \hat{s}_{j_r} \cdots s_{j_k}$ implies (cancelling s_{i_1}) that $s_{j_1} \cdots s_{j_k} = s_{j_1} \cdots \hat{s}_{j_q} \cdots \hat{s}_{j_r} \cdots s_{j_k}$. So $\ell(s_{j_1} \cdots s_{j_k}) < k$, and $s_{j_1} \cdots s_{j_k}$ is not a reduced expression. Hence, a contradiction.

We conclude that case (ii) is the only possibility. The identity $s_{i_1} s_{j_1} \cdots s_{j_k} = s_{j_1} \cdots \hat{s}_{j_q} \cdots s_{j_k}$ can be rewritten

$$\varphi = s_{j_1} \cdots s_{j_k} = s_{i_1} s_{j_1} \cdots \hat{s}_{j_q} \cdots s_{j_k}. \qquad \blacksquare$$

Arbitrary Reflection Groups We now begin the proof of Proposition 23-3 for an arbitrary W. The proof is by induction on length. The cases of length 0 or 1 are trivial. We assume that Proposition 23-3 holds for elements from W of length $< k$. Consider two reduced expressions

$$s_{i_1} \cdots s_{i_k} = s_{j_1} \cdots s_{j_k}$$

for $\varphi \in W$.

Case I $s_{i_1} = s_{j_1}$.

Cancelling, $s_{i_2} \cdots s_{i_k} = s_{j_2} \cdots s_{j_k}$. By induction, $\Delta_{i_2} \cdots \Delta_{i_k} = \Delta_{j_2} \cdots \Delta_{j_k}$. Since $\Delta_{i_1} = \Delta_{j_1}$, we also have $\Delta_{i_1} \cdots \Delta_{i_k} = \Delta_{j_1} \cdots \Delta_{j_k}$.

Case II $s_{i_k} = s_{j_k}$.

The argument is analogous to that in Case I.

Case III: General Case By Case I, we can assume $s_{i_1} \neq s_{j_1}$. For notational convenience, we shall let

$$s = s_{i_1} \quad \text{and} \quad t = s_{j_1}.$$

We shall show that, if $\Delta_{i_1} \cdots \Delta_{i_k} \neq \Delta_{j_1} \cdots \Delta_{j_k}$, then φ belongs to

$$W_{s,t} = \langle s, t \mid s^2 = t^2 = (st)^k = 1 \rangle$$

and has two reduced expressions

$$(*) \qquad sts \cdots = \varphi = tst \cdots \quad (k \text{ terms in each expression})$$

such that the two corresponding Δ operations satisfy the inequality

$$(**) \qquad \Delta_s \Delta_t \Delta_s \cdots \neq \Delta_t \Delta_s \Delta_t \cdots .$$

This contradicts what we have already observed about the dihedral reflection-group case. To prove $(*)$ and $(**)$, we shall produce, by induction, a string of reduced expressions for φ

$$(*') \qquad \begin{aligned} ss_{i_2} \cdots s_{i_k} &= t(s_{j_2} \cdots s_{j_k}) = st(s_{j_2} \cdots s_{j_{k-1}}) = tst(s_{j_2} \cdots s_{j_{k-2}}) = \cdots \\ &= sts \cdots (k \text{ terms}) = tst \cdots (k \text{ terms}), \end{aligned}$$

where the corresponding Δ operators satisfy the inequalities

$$(**') \qquad \begin{aligned} \Delta_s(\Delta_{i_2} \cdots \Delta_{i_k}) &\neq \Delta_t(\Delta_{i_2} \cdots \Delta_{j_k}) \neq \Delta_s\Delta_t(\Delta_{j_2} \cdots \Delta_{j_{k-1}}) \\ &\neq \Delta_t\Delta_s\Delta_t(\Delta_{j_2} \cdots \Delta_{j_{k-2}}) \neq \cdots \\ &\neq \Delta_s\Delta_t\Delta_s \cdots (k \text{ terms}) \neq \Delta_t\Delta_s\Delta_t \cdots (k \text{ terms}). \end{aligned}$$

Observe that $(*)$ is the last equality of $(*')$, whereas $(**)$ is the last inequality of $(**')$. The equalities of $(*')$ and the inequalities of $(**')$ are obtained by an inductive argument. Each equality or inequality is obtained from the previous one. Observe that the initial line of both $(*')$ and $(**')$ are our operating hypotheses. As an example of the inductive argument, we shall demonstrate how to deduce the second lines of $(*')$ and $(**')$ from the first lines. The argument for subsequent lines is similar.

We assume that $ss_{i_2} \cdots s_{i_k} = ts_{j_2} \cdots s_{j_k}$ and $\Delta_s\Delta_{i_2} \cdots \Delta_{i_k} \neq \Delta_t\Delta_{j_2} \cdots \Delta_{j_k}$. The previous lemma, along with the assumption that $s \neq t$, tells us that $sts_{j_2} \cdots \hat{s}_{j_q} \cdots s_{j_k}$ is also a reduced expression for φ. So $ss_{i_2} \cdots s_{i_k} \neq ts_{j_2} \cdots s_{j_k} = sts_{j_2} \cdots \hat{s}_{j_q} \cdots s_{j_k}$. By Case I

$$\Delta_s\Delta_{i_2} \cdots \Delta_{i_k} = \Delta_s\Delta_t\Delta_{j_2} \cdots \hat{\Delta}_{j_q} \cdots \Delta_{j_k}.$$

If $q < k$, then, by Case II,

$$\Delta_t \Delta_{j_2} \cdots \Delta_{j_k} = \Delta_s \Delta_t \Delta_{j_2} \cdots \hat{\Delta}_{j_q} \cdots \Delta_{j_k}.$$

From the last two identities, we would have

$$\Delta_s \Delta_{i_2} \cdots \Delta_{i_k} = \Delta_t \Delta_{j_2} \cdots \Delta_{j_k},$$

contradicting our hypothesis. So the only possibility is $q = k$. Thus we must have

$$ts_{j_2} \cdots s_{j_k} = sts_{j_2} \cdots \hat{s}_{j_q} \cdots s_{j_k}.$$

Also,

$$\Delta_t \Delta_{j_2} \cdots \Delta_{j_k} \neq \Delta_s \Delta_t \Delta_{j_2} \cdots \hat{\Delta}_{j_q} \cdots \Delta_{j_k}.$$

Otherwise, as above, we would have a contradiction.

24 Representations of pseudo-reflection groups

In this chapter, we discuss some unique features of the representation theory of pseudo-reflection groups. In particular, we discuss the relation between the representation theory and the invariant theory of pseudo-reflection groups.

24-1 S_G as the regular representation

We assume that V is a finite dimensional vector space over a field $\mathbb{F}$, and that $G \subset \mathrm{GL}(V)$ *is a finite nonmodular pseudo-reflection group*. Besides $S = S(V)$, we shall also be using the following notation.

$$R = S^G, \quad \text{the ring of invariants of } G$$

$$I = \text{the graded ideal of } S \text{ generated by } \sum_{i \geq 1} R_i$$

$$S_G = S/I, \quad \text{the ring of covariants of } G.$$

Since the action of G on S maps I to itself, it follows that there is an induced action of G on S_G.

Definition: A G module N over $\mathbb{F}$ is the *regular representation* of G if there exists $x \in N$ such that $\{\varphi \cdot x \mid \varphi \in G\}$ is an $\mathbb{F}$ basis of N.

So G acts on N by permuting the basis $\{\varphi \cdot x \mid \varphi \in G\}$. There is a standard situation in which regular representations arise. The normal basis theorem in Galois theory (see §12 of Chapter VIII of Lang [1]) tells us that, in the case of a Galois extension $\mathbb{F} \subset E$, the action of the Galois group G on the $\mathbb{F}$ vector space E gives the regular representation of G. The regular representation is further discussed in Appendix B. In this section, we want to show that:

Theorem *S_G gives the regular representation of G.*

By Corollary 23-1, we have

$$\dim_{\mathbb{F}} S_G = |G|.$$

So S_G has the right dimension to be the regular representation of G. We begin by demonstrating that the regular representation of G arises naturally, via Galois theory, from the inclusion $R \subset S$. We must pass to fraction fields. Since $R \subset S$ are integral domains, we can form their fraction fields $F(R) \subset F(S)$.

Since G is nonmodular, we have:

Lemma A $F(R) = F(S)^G$.

Proof We obviously have $F(R) \subset F(S)^G$. Consider $w = x/y \in F(S)^G$, where $x, y \in S$. (We are using the convenient notation x/y to denote xy^{-1}.) We want to

show that we can choose $x, y \in R$. It suffices to show that we can choose $y \in R$, since this forces $wy \in F(S)^G$. Thus $x = wy \in S \cap F(S)^G = R$.

Now, since char $\mathbb{F}$ does not divide $|G|$, we can apply the averaging operator $\text{Av}: S \to S$ from Chapter 14 and obtain

$$w = \text{Av}(w) = \text{Av}\left(\frac{x}{y}\right) = \frac{1}{|G|}\sum_{\varphi \in G}\frac{\varphi \cdot x}{\varphi \cdot y} = \frac{1}{|G|}\frac{z}{\prod_{\varphi \in G}\varphi \cdot y}$$

for some $z \in S$. Since G permutes the set $\{\varphi \cdot y \mid \varphi \in G\}$, we have $[\prod_{\varphi \in G}\varphi \cdot y] \in R$. ■

Next, we introduce some ideas from Galois theory. The identity $F(R) = F(S)^G$ tells us that $F(S)$ is a Galois extension of $F(R)$ of degree $|G|$. In particular, by the normal basis theorem of Galois theory, G acts on the $F(R)$ vector space $F(S)$ as the regular representation.

Since G maps I to itself, it follows from Maschke's theorem in Appendix B that we can find a G subspace $M_G \subset S$ such that

$$S = I \oplus M_G.$$

Then $M_G \cong S_G$ as G modules and it suffices to show that M_G gives the regular representation. We shall do so by moving to a larger field $\mathbb{F} \subset \mathcal{F}$, where it is clear that the induced action of G on $M_G \otimes_{\mathbb{F}} \mathcal{F}$ gives the regular representation. The existence of such a field $\mathcal{F}$ follows from Lemma A plus:

Lemma B $F(S) = M_G \otimes_{\mathbb{F}} F(R)$.

Proof It follows from §18-3 that S is a free R module generated by any $\mathbb{F}$ basis of M_G. In other words,

$$S = M_G \otimes_{\mathbb{F}} R$$

as R modules. This identity extends to that given in the lemma. For, let $\mathcal{B}$ be an $\mathbb{F}$ basis of M_G. By the above results from §18-3, the elements of $\mathcal{B}$ are linearly independent over R. Consequently, they are also linearly independent over $F(R)$. Since $\dim_{F(R)} F(S) = |G| = |\mathcal{B}|$, it follows that $\mathcal{B}$ is a $F(R)$ basis of $F(S)$. ■

The identity in Lemma B is G equivariant, i.e., the action of G on $F(S)$ and on $M_G \otimes_{\mathbb{F}} F(R)$ correspond via this identity. Consequently, G acts on $M_G \otimes_{\mathbb{F}} F(R)$ as the regular representations over $F(R)$. It follows that G acts on M_G as the regular representation over $\mathbb{F}$ because characters completely determine representations in the nonmodular case. And, by the above, the character $\chi: G \to \mathbb{F}$ associated with the action of G on M_G is that of the regular representation.

24-2 The Poincaré series of irreducible representations

Let $M = \bigoplus_{i=0}^{\infty} M_i$ be a graded connected $\mathbb{F}$ vector space, and suppose that the group G acts on M so as to preserve the homogeneous components $\{M_i\}$. Each M_i is then a representation of G. As outlined in Appendix B, every representation

of G can be decomposed as a direct sum of irreducible representations, and the number of copies of each irreducible representation in such a decomposition is unique.

Let $\phi\colon G \longrightarrow \mathrm{GL}_n(\mathbb{F})$ be an irreducible representation of G. We can define the Poincaré series of M (with respect to ϕ) as follows.

Definition: $P_\phi(M) = \sum_{i=0}^{\infty} a_i t^i$, where a_i = the number of occurrences of the representation ϕ in M_i.

In this section we obtain formulas for $P_\phi(M)$ for the cases $M = S$ and $M = S_G$. Let $\chi\colon G \longrightarrow \mathbb{F}$ be the associated character of ϕ.

***Theorem* (Generalized Molien's Theorem)** *Given a finite nonmodular group $G \subset \mathrm{GL}(V)$, then*

$$P_\phi(S) = \frac{1}{|G|}\sum_{\varphi\in G}\frac{\chi(\varphi)}{\det(1-\varphi t)}.$$

This theorem is a direct generalization of Molien's Theorem because, if we take the trivial representation of G, then $P_\phi(S) = P_t(S^G)$. Moreover, since $\chi(\varphi) = 1$ in this case for all $\varphi \in G$, the above theorem is exactly Molien's identity

$$P_t(S^G) = \frac{1}{|G|}\sum_{\varphi\in G}\frac{1}{\det(1-\varphi t)}$$

as given in §17-2. We can deduce from the generalized Molien's theorem the following identity for pseudo-reflection groups.

Corollary *Given a finite nonmodular pseudo-reflection group $G \subset \mathrm{GL}(V)$, then*

$$P_\phi(S_G) = \left[\prod_{i=1}^{n}(1-t^{d_i})\right]\frac{1}{|G|}\sum_{\varphi\in G}\frac{\chi(\varphi)}{\det(1-\varphi t)}.$$

Proof of Theorem The proof of the generalized Molien's Theorem is an extension of the proof of Molien's Theorem as given in §17-2. If $\varphi\colon V \longrightarrow V$ is a linear map, we shall use

$$\varphi_i\colon S_i \longrightarrow S_i$$

to denote the induced maps on the homogeneous components of $S = \bigoplus_{i=0}^{\infty} S_i$. We have the trace formula

$$\sum_{i=0}^{\infty}\mathrm{tr}(\varphi_i)t^i = \frac{1}{\det(1-\varphi t)}$$

given in Proposition 17-2A. Next, let

σ_i = the character of the representation given by the action of G on S_i.

Let ϕ be an irreducible representation with character χ. For any character $\lambda\colon G \to \mathbb{F}$ corresponding to a representation $\rho\colon G \to \mathrm{GL}(V)$, the number of occurrences of ϕ in ρ is given by the inner product

$$(\chi, \lambda) = \frac{1}{|G|} \sum_{\varphi \in G} \chi(\varphi)\lambda(\varphi)^{-1}.$$

In particular $a_i = (\chi, \sigma_i)$ and, so, we have the series of identities

$$\begin{aligned} P_\phi(S) &= \sum_{i=0}^{\infty} (\chi, \sigma_i) t^i = \sum_{i=0}^{\infty} \frac{1}{|G|} \sum_{\varphi \in G} \chi(\varphi)\sigma_i(\varphi)^{-1} t^i \\ &= \frac{1}{|G|} \sum_{\varphi \in G} \chi(\varphi) \Big[\sum_{i=0}^{\infty} \sigma_i(\varphi)^{-1}\Big] = \frac{1}{|G|} \sum_{\varphi \in G} \frac{\chi(\varphi)}{\det(1 - \varphi t)}. \end{aligned}$$ ∎

Proof of Corollary The isomorphism $S = M_G \otimes R$ of G modules obtained in §24-1, plus the fact that G acts trivially on R, tells us that

$$P_\phi(S) = P_\phi(M_G) P_t(R).$$

The generalized Molien formula for $P_\phi(S)$, along with the identity $P_t(R) = \prod_{i=1}^{n} \frac{1}{1-t^{d_i}}$, gives the corollary for $P_\phi(M_G)$. Since $M_G \cong S_G$ as G modules, the corollary also holds for $P_\phi(S_G)$. ∎

24-3 Exterior powers of reflection representation

In this section, we consider irreducible essential complex pseudo-reflection groups $G \subset \mathrm{GL}(V)$ such that G is generated by n reflections $\{s_1, \dots, s_n\}$, where $n = \dim_{\mathbb{C}} V$. Not every irreducible essential complex pseudo-reflection group satisfies this hypothesis. As mentioned in §20-2, some irreducible complex pseudo-reflection groups acting on an n-dimensional vector space V require $n+1$ pseudo-reflections to generate them. However, all finite Euclidean reflection groups (when we consider them as complex pseudo-reflection groups) satisfy the hypothesis. A complete list of the n-dimensional irreducible essential pseudo-reflection groups which are generated by n pseudo-reflections is given in Chapter 12 of Shephard-Todd [1].

The exterior powers $\{E_k(V)\}$ of V were defined in §22-2. We now prove that, given an irreducible reflection group as above, when we consider the naturally induced action of G on the exterior powers $\{E_k(V)\}$, then:

***Theorem A* (Steinberg)** *The exterior powers $\{E_0(V), E_1(V), \dots, E_n(V)\}$ give distinct irreducible representations of G.*

This result appears as an exercise in Bourbaki [1]. For notational convenience, let

$$\lambda_k = \text{the representation given by the } G \text{ module } E_k(V).$$

Since $E_k(V)$ is irreducible, we can define the Poincaré series $P_{\lambda_k}(S_G)$ of λ_k as in §24-2. Moreover, we can use Solomon's arguments from Chapter 22 to explicitly calculate $P_{\lambda_k}(S_G)$. Letting $\{m_1, \ldots, m_n\}$ be the exponents of G, then, for each of the cases $1 \leq k \leq n$, we have:

Theorem B $P_{\lambda_k}(S_G) = \sum_{i_1 < \cdots < i_k} t^{m_{i_1} \cdots m_{i_k}}$.

In particular, in the case $\lambda = \lambda_1$ we have:

Corollary $P_\lambda(S_G) = t^{m_1} + t^{m_2} + \cdots + t^{m_n}$.

The rest of this section will be devoted to the proof of the above theorems. Granted previous results, the proof of Theorem B is quite simple, and so will be given first.

Proof of Theorem B The proof of Theorem B is based on the Solomon identity

$$(*) \qquad \prod_{i=1}^{n}(1 + Yt^{m_i}) = \left[\prod_{i=1}^{n} 1 - t^{d_i}\right] \frac{1}{|G|} \sum_{\varphi \in G} \frac{\det(1 + \varphi Y)}{\det(1 - \varphi t)}$$

from §22-4. Let $\phi_k =$ the character of the representation λ_k. We can write

$$(**) \qquad \det(1 + \varphi Y) = 1 + \phi_1(\varphi)Y + \phi_2(\varphi)Y^2 + \cdots + \phi_n(\varphi)Y^n.$$

This identity is an analogue for $E(V)$ of Proposition 17-2A. It has already appeared in the proof of Proposition 22-4.

If we substitute $(**)$ into $(*)$ and use the definition of $P_{\lambda_k}(S_G)$ given by Corollary 24-2, then $(*)$ can be rewritten

$$\prod_{i=1}^{n}(1 + Yt^{m_i}) = \sum_{i=0}^{\infty} P_{\lambda_k}(S_G)Y^k.$$

The theorem now follows.

Proof of Theorem A As indicated above, we shall assume that $G \subset \mathrm{GL}(V)$ is an irreducible essential pseudo-reflection group generated by n reflections $\{s_1, \ldots, s_n\}$, where $n = \dim_{\mathbb{C}} V$. For each s_i, choose its exceptional eigenvector e_i. So $s_i \cdot e_i = \xi e_i$, where ξ is a root of unity. As explained in §14-1, we can represent s_i in the form

$$s_i \cdot x = x + (\xi - 1)\frac{(e_i, x)}{(e_i, e_i)} e_i,$$

where $(\ ,\ )$ is a positive definite Hermitian form invariant under G, i.e., $(\varphi \cdot x, \varphi \cdot y) = (x, y)$ for all $x, y \in V$ and $\varphi \in G$. So $s_i \cdot e_j = e_j$ if and only if e_i and e_j are orthogonal.

The Graph of G Let $G \subset \mathrm{GL}(V)$ be an essential pseudo-reflection group generated by n reflections $\{s_1, \dots, s_n\}$, where $n = \dim_{\mathbb{C}} V$. We can represent the orthogonality relations between the vectors $\{e_1, \dots, e_n\}$ by a graph consisting of n vertices $\{e_1, \dots, e_n\}$ with an edge between i and j if $(e_i, e_j) \neq 0$, i.e., if e_i and e_j are not orthogonal. The irreducibility of G is characterized in terms of this graph.

Proposition *Γ is connected if and only if $G \subset \mathrm{GL}(V)$ is an irreducible representation.*

If the graph is not connected, then the vectors $\{e_i\}$ from each connected component of the graph generate a subspace of V invariant under G. When the graph is connected, the irreducibility of the action of G follows from:

Lemma *Suppose $W \subset V$ is stable under s_i. Then its orthogonal complement $W^{\perp}$ is stable under s_i. Moreover, $e_i \in W$ or $e_i \in W^{\perp}$, but not both.*

Proof The relation $(s_i \cdot x, y) = (x, s_i^{-1} \cdot y)$ for all $x, y \in V$ tells us that $W^{\perp}$ is stable under s_i^{-1}. So $W^{\perp}$ is also stable under s_i. Regarding e_i, if we decompose $e_i = \alpha + \beta$ corresponding to the decomposition $V = W \oplus W^{\perp}$, then $s_i \cdot \alpha = \xi\alpha$ and $s_i \cdot \beta = \xi\beta$. If both α and β are nonzero, then they are linearly independent. This contradicts the fact that $\mathrm{rank}(1 - s_i) = 1$. So $\alpha = 0$ or $\beta = 0$. ∎

The proof of Theorem A will be by induction on $n = \dim_{\mathbb{C}} V$. Let Γ be the graph of $G \subset \mathrm{GL}(V)$ as discussed above. Pick a vertex in Γ such that Γ is still connected when we delete the vertex. Without loss of generality, assume that e_n is the vertex. Let

$$W = \text{the subspace of } V \text{ spanned by } \{e_1, \dots, e_{n-1}\}$$

$$H = \text{the reflection subgroup of } W \text{ generated by } \{s_1, \dots, s_{n-1}\}.$$

By induction, we can assume that $H \subset \mathrm{GL}(W)$ has distinct irreducible exterior powers $\{E_k(W)\}$.

Consider $E_k(V)$ as an H module. Then $E_k(W) \subset E_k(V)$ is a submodule. For future use, we record that $E_k(W)$ has a basis

$$\mathcal{B} = \{e_{i_1} \wedge \cdots \wedge e_{i_k} \mid i_1 < \cdots < i_k \leq n-1\},$$

while $E_k(V)$ has a basis $\mathcal{B} \coprod \mathcal{C}$, where

$$\mathcal{C} = \{e_{i_1} \wedge \cdots \wedge e_{i_{k-1}} \wedge e_n \mid i_1 < \cdots < i_{k-1} \leq n-1\}.$$

In particular, $\mathcal{C}$ projects to a basis of the quotient module $E_k(V)/E_k(W)$. Observe that we have an isomorphism of H modules

$$E_k(V)/E_k(W) \cong E_{k-1}(W)$$

$$e_{i_1} \wedge \cdots \wedge e_{i_{k-1}} \wedge e_n \leftrightarrow e_{i_1} \wedge \cdots \wedge e_{i_{k-1}}.$$

In particular, the quotient module $E_k(V)/E_k(W)$ is an irreducible H module. We now set about proving that the representations $\{E_k(V)\}$ are irreducible and distinct.

(i) Irreducible Suppose that we have a G submodule $\{0\} \neq M \subset E_k(V)$. We want to show that $M = E_k(V)$. The irreducibility of $E_k(W)$ tells us that either $E_k(W) \cap M = \{0\}$ or $E_k(W) \subset M$. Similarly, if M' is a G module such that

$$E_k(V) = M \oplus M',$$

then either $E_k(W) \cap M' = \{0\}$ or $E_k(W) \subset M'$.

Lemma A *If $E_k(W) \subset M$, or $E_k(W) \subset M'$, then $M = E_k(V)$.*

Proof We shall only do the case $E_k(W) \subset M$. First of all,

$$E_k(W) \neq M$$

because M is invariant under G. But $E_k(W)$ is not. To see this, consider s_n. Pick e_q, where $q < n$ and $(e_q, e_n) \neq 0$. Then

$$s_n \cdot e_q = e_q + \alpha e_n, \quad \text{where } \alpha \neq 0$$

If $e_{i_1} \wedge \cdots \wedge e_{i_k} \in \mathcal{B}$ involves e_q, then $s_n(e_{i_1} \wedge \cdots \wedge e_{i_k}) = (s_n \cdot e_{i_1}) \wedge \cdots \wedge (s_n \cdot e_{i_k})$ involves $e_{i_1} \wedge \cdots \wedge \hat{e}_q \wedge \cdots \wedge e_{i_k} \wedge e_n \in \mathcal{C}$ when expanded in terms of $\mathcal{B} \coprod \mathcal{C}$ ("$\wedge$" denotes elimination).

So M has a nontrivial image in $E_k(V)/E_k(W)$. Since the quotient module is an irreducible H module, it follows that the image of M is all of $E_k(V)/E_k(W)$. Thus $M = E_k(V)$. ∎

To complete the proof of the theorem, we need only show:

Lemma B *It is not possible to have both $E_k(W) \cap M = \{0\}$ and $E_k(W) \cap M' = \{0\}$.*

Proof First of all, these conditions imply that both M and M' would imbed in $E_k(V)/E_k(W) \cong E_{k-1}(W)$. Since $E_{k-1}(W)$ is irreducible as an H module, we must then have

$$M \cong E_{k-1}(W) \cong M'$$

as H modules. Since $E_k(V) = M \oplus M'$, we have

$$\dim_{\mathbf{C}} E_k(V) = \dim_{\mathbf{C}} M + \dim_{\mathbf{C}} M'.$$

On the other hand,

$$\dim_{\mathbf{C}} E_k(V) = \dim_{\mathbf{C}} E_k(W) + \dim_{\mathbf{C}} E_{k-1}(W) = \dim_{\mathbf{C}} E_k(W) + \dim_{\mathbf{C}} M.$$

These identities force

$$\dim_{\mathbf{C}} E_k(W) = \dim_{\mathbf{C}} M'.$$

Hence, by counting dimensions, the imbedding $E_k(W) \to E_k(V)/M \cong M'$ is an isomorphism

$$E_k(W) \cong M'$$

of H modules. We now know that $E_k(W) \cong M' \cong E_{k-1}(W)$ as H modules, which contradicts the assumption that the H modules $\{E_k(W)\}$ are all distinct.

(ii) Distinct Since $\dim_{\mathbb{C}} E^k(V) = \binom{n}{k}$, we can distinguish all the modules except for $E_k(V)$ and $E_{n-k}(V)$ on the basis of dimension. For any $1 \leq i \leq n$, let $\phi_i : G \to \mathbb{C}$ be the character of the G module $E_i(V)$. To distinguish $E_k(V)$ and $E_{n-k}(V)$, it suffices to find $\varphi \in G$ such that $\phi_k(\varphi) \neq \phi_{n-k}(\varphi)$. Let φ be a reflection. We have the identity

$$\sum \phi_i(\varphi)t^i = \det(1 + \varphi t) = (1 + \omega t)(1 + t)^{n-1},$$

where ω is the exceptional eigenvalue of φ. The first equality has already been mentioned above in the proof of Theorem B. The second equality is straightforward. Next, by comparing coefficients on both sides of the equation, we obtain

$$\phi_k(\varphi) = \binom{n-1}{k} + \binom{n-1}{k-1}\omega$$

$$\phi_{n-k}(\varphi) = \binom{n-1}{n-k} + \binom{n-1}{n-k-1}\omega.$$

So $\phi_k \neq \phi_{n-k}$. ■

24-4 MacDonald representations

Sub pseudo-reflection groups of $G \subset \mathrm{GL}(V)$ can be used to induce irreducible representations of G. Let $H \subset G \subset \mathrm{GL}(V)$ be such a subgroup. As in §20-2, decompose each reflection $s \in H$ as

$$s \cdot x = x + \Delta_s(x)\alpha_s$$

and form the element

$$\Omega_H = \prod_s \alpha_s$$

belonging to $S_N(V)$, where $N =$ the number of reflections in H. It follows from Propositions A and B of §20-2 that the one-dimensional space $\mathbb{F}\Omega_H$ gives the *skew representation* of H, i.e.,

$$\varphi \cdot \Omega_H = (\det \varphi)^{-1}\Omega_H$$

for all $\varphi \in H$. Moreover, N is the lowest degree at which the skew representation occurs in $S(V)$. Let

$$W_H = \text{the } G \text{ module generated by } \mathbb{F}\Omega_H.$$

Then we have:

Proposition

(i) *W_H is an irreducible representation of G;*
(ii) *The representation W_H does not occur in $S(V)$ in degree $< N$;*
(iii) *The representation W_H occurs in $S_N(V)$ with multiplicity* 1.

Proof Regarding (ii) and (iii), we know that, if we restrict from G to H, then W_H contains a copy of the skew representation of H. However, $S_i(V)$ contains no copies of the skew representation for $i < N$, and only one copy when $i = N$. Regarding assertion (i), suppose $W_H = M \oplus M'$ as a G module. We want to show that either $M = W_H$ or $M' = W_H$. We claim that

$$\Omega_H \in M \quad \text{or} \quad \Omega_H \in M'.$$

Write $\Omega_H = x+y$, where $x \in M$ and $y \in M'$. Given $\varphi \in H$, $\varphi \cdot \Omega_H = (\det \varphi)^{-1}\Omega_H$ implies that $\varphi \cdot x = (\det \varphi)^{-1}x$ and $\varphi \cdot y = (\det \varphi)^{-1}y$. So if $x \neq 0$ and $y \neq 0$, we should have two copies of the skew representation of H in W_H. But, as already observed, the skew representation occurs only once in $S_N(V)$. We conclude that $x = 0$ or $y = 0$.

Without loss of generality, assume that $\Omega_H \in M$. Then, by the definition of Ω_H, $W_H \subset M$, i.e., $W_H = M$ and $M' = 0$. ∎

A representation constructed as above is called a *MacDonald representation.* This construction was first discussed in MacDonald [1]. It was further analyzed in Lusztig [1] and Lusztig [2].

Example: The canonical examples of MacDonald representations occur in the case of the symmetric group $W(A_\ell) = \Sigma_{\ell+1}$. It is a standard fact that the irreducible representations of $\Sigma_{\ell+1}$ are indexed by the partitions of $\ell + 1$. The MacDonald construction provides a construction of these representations. For each partition $n_1 + \cdots + n_k = \ell + 1$, we have the reflection subgroup

$$\Sigma_{n_1} \times \cdots \times \Sigma_{n_k} \subset \Sigma_{\ell+1}.$$

Here $\Sigma_{\ell+1}$ is generated by the fundamental reflections $\{s_1, \ldots, s_\ell\}$, where $s_i =$ the permutation $(i, i + 1)$. And the factor Σ_{n_j} of $\Sigma_{\ell+1}$ is generated by $\{s_i \mid n_1 + \cdots + n_{j-1} < i < n_1 + \cdots + n_j\}$. So $\Sigma_{n_1} \times \cdots \times \Sigma_{n_k}$ is a reflection subgroup and we can apply the MacDonald construction to obtain an irreducible representation of $\Sigma_{\ell+1}$.

25 Harmonic elements

In this section, we introduce the concept of the harmonic elements of a group $G \subset \mathrm{GL}(V)$. Before defining harmonic elements, we first introduce the algebra of differential operators. This is done in §25-2, after a discussion of Hopf algebras in §25-1. Harmonic elements are defined in §25-4. Harmonic elements will be studied in detail in Chapter 26. In particular, it will be demonstrated that the property of G being a pseudo-reflection group can be characterized in terms of harmonic elements. This chapter is designed to introduce the machinery necessary for that study.

25-1 Hopf algebras

In this chapter, we assume that $\mathbb{F}$ *is a field of characteristic zero*, and that V is a finite dimensional vector space over $\mathbb{F}$. Let

$$S = S(V) \quad \text{and} \quad S^* = S(V^*).$$

Before defining the harmonic elements of $S = S(V)$, we need to discuss the various relations of S^* to S. That will be done in this section, as well as in §25-2 and §25-3. The reason for assuming that $\mathbb{F}$ is of characteristic zero is to enable us to define the bilinear pairing $\langle -, - \rangle : S^* \otimes S \to \mathbb{F}$ described in part (b) of this section.

(a) Hopf Algebras We can consider S and S^* as graded Hopf algebras. A basic reference for graded Hopf algebras is Milnor-Moore [1]. A *graded Hopf algebra H* is a graded connected vector space over $\mathbb{F}$ with structure maps

$$H \xrightarrow{\Delta} H \otimes H \xrightarrow{\mu} H$$

such that

(i) H is an associative algebra $H \otimes H \xrightarrow{\mu} H$ with unit;

(ii) H is a coassociative coalgebra $H \xrightarrow{\Delta} H \otimes H$ with counit. This means that, for every element $x \in H$, the coproduct is of the form

$$\Delta(x) = x \otimes 1 + 1 \otimes x + \sum_i x' \otimes x'', \quad \text{where } \deg x' > 0 \text{ and } \deg x'' > 0$$

and we have the identity

$$(\Delta \otimes 1)\Delta(x) = (1 \otimes \Delta)\Delta(x);$$

(iii) The algebra and coalgebra structures are compatible in the sense that the following identity is satisfied

$$\Delta(xy) = \Delta(x)\Delta(y)$$

for all $x, y \in H$. In other words, Δ is an algebra map.

Regarding the algebra structure, both S and S^* are polynomial algebras. If $\{t_1, \ldots, t_n\}$ is a basis of V, and $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of V^*, then we can write

$$S = \mathbb{F}[t_1, \ldots, t_n] \quad \text{and} \quad S^* = \mathbb{F}[\alpha_1, \ldots, \alpha_n].$$

The coalgebra structures

$$\Delta\colon S \to S \otimes S \quad \text{and} \quad \Delta^*\colon S^* \to S^* \otimes S^*$$

are determined by stipulating that the elements of V and V^* are *primitive*, i.e.,

$$\Delta(x) = x \otimes 1 + 1 \otimes x \quad \text{for all } x \in V$$
$$\Delta^*(\alpha) = \alpha \otimes 1 + 1 \otimes \alpha \quad \text{for all } \alpha \in V^*.$$

S and S^* are said to be *primitively generated* Hopf algebras.

(b) Duality The Kronecker pairing

$$\langle \_, \_ \rangle\colon V^* \otimes V \to \mathbb{F}$$

extends to a pairing

$$\langle \_, \_ \rangle\colon S^* \otimes S \to \mathbb{F},$$

which relates the Hopf algebra structures of S^* and S. This extended pairing is determined by the rule

$$(*) \qquad \langle \alpha, xy \rangle = \langle \Delta^*(\alpha), x \otimes y \rangle$$

for any $\alpha \in S^*$ and $x, y \in S$. Observe that this is actually a recursive formula. If $\Delta(\alpha) = \sum_i \alpha' \otimes \alpha''$, then

$$\langle \alpha, xy \rangle = \sum_i \langle \alpha', x \rangle \langle \alpha'', y \rangle.$$

We can, thereby, obtain explicit formulas for the pairing $\langle \_, \_ \rangle$. As before, write $S = \mathbb{F}[t_1, \ldots, t_n]$ and $S^* = \mathbb{F}[\alpha_1, \ldots, \alpha_n]$, where $\{t_1, \ldots, t_n\}$ and $\{\alpha_1, \ldots, \alpha_n\}$ are dual bases of V and V^*, respectively. Then S and S^* have canonical bases

$$\{t^E = t_1^{e_1} \cdots t_k^{e_k}\} \quad \text{and} \quad \{\alpha^F = \alpha_1^{f_1} \cdots \alpha_k^{f_k}\},$$

where $E = (e_1, e_2, \ldots)$ and $F = (f_1, f_2, \ldots)$ range over all sequences of nonnegative integers with only finitely many nonzero terms. The pairing satisfies:

Lemma $\langle \alpha^E, t^F \rangle = \begin{cases} E! & \text{if } E = F \\ 0 & \text{if } E \neq F \end{cases}$ *where* $E! = \prod e_s!$.

Proof To prove this, we use $(*)$ and the coproduct formula for $\Delta^*\colon S^* \longrightarrow S^* \otimes S^*$

$$\Delta(\alpha^E) = \sum_{F+G=E} (F, G)\alpha^F \otimes \alpha^G,$$

where

$$(F, G) = \frac{E!}{F!\,G!}. \qquad \blacksquare$$

Finally, under the pairing $\langle -, - \rangle$, S^* and S are dual Hopf algebras. In other words, the maps

$$\mu\colon S \otimes S \to S \quad \text{and} \quad \Delta\colon S \to S \otimes S$$

dualize to give the maps

$$\Delta^*\colon S^* \to S^* \otimes S^* \quad \text{and} \quad \mu^*\colon S^* \otimes S^* \to S^*,$$

respectively. Notably, the duality relation $(*)$ can be rewritten as

$$\langle \alpha, \mu(x \otimes y) \rangle = \langle \Delta^*(\alpha), x \otimes y \rangle,$$

which gives the duality between μ and Δ^*.

25-2 Differential operators

We continue to use the notation of §25-1. Besides thinking of S^* as the dual Hopf algebra of S, we can also interpret S^* as a Hopf algebra of *differential operators* acting on S. For any $\alpha \in S^*$, we use

$$D_\alpha\colon S \to S$$

to denote the corresponding linear operator. We give three different approaches to the action $S^* \otimes S \to S$.

(a) First Approach We begin with a relatively informal description of the action $S^* \otimes S \to S$. For any $\alpha \in V^*$, the operator D_α is a derivation determined by the rules:

$$\text{(E-1)} \qquad \begin{aligned} D_\alpha(x) &= \langle \alpha, x \rangle \quad \text{for } x \in V \\ D_\alpha(xy) &= D_\alpha(x)y + xD_\alpha(y) \quad \text{for } x, y \in S. \end{aligned}$$

For an arbitrary $\alpha \in S^* = \mathbb{F}[\alpha_1, \ldots, \alpha_n]$, we define D_α by replacing $\{\alpha_1, \ldots, \alpha_n\}$ in $\alpha = f(\alpha_1, \ldots, \alpha_n)$ by the derivatives $\{D_{\alpha_1}, \ldots, D_{\alpha_n}\}$. In other words, multiplication in S^* corresponds to composition of the associated differential operators.

(b) Second Approach More formally, the action $S^* \otimes S \to S$ is determined by the two requirements that:

(E-2) For any $\alpha \in V^*$ and $x \in V$, $D_\alpha(x) = \langle \alpha, x \rangle$;
(E-3) For any $\alpha \in S^*$ and $x, y \in S$, if $\Delta^*(\alpha) = \sum_i \alpha_i' \otimes \alpha_i''$, then

$$D_\alpha(xy) = \sum D_{\alpha_i'}(x) D_{\alpha_i''}(y).$$

This definition of D_α agrees with the previous one. First of all, for $\alpha \in V^*$ we have $\Delta^*(\alpha) = \alpha \otimes 1 + 1 \otimes \alpha$. So it follows from property (E-3) that D_α is a derivation. Secondly, it follows from property (E-3) and the identity $\Delta^*(\alpha\beta) = \Delta^*(\alpha)\Delta^*(\beta)$, that $D_\alpha D_\beta = D_{\alpha\beta}$ for any $\alpha, \beta \in S^*$.

(c) Third Approach There is also a third way to define the operations D_α. We can use the above defining properties to deduce the following formula for D_α.

Lemma A *Given $\alpha \in S^*$ and $x \in S$, if $\Delta(x) = \sum_i x_i' \otimes x_i''$, then*

$$D_\alpha(x) = \sum_i \langle \alpha, x_i' \rangle x_i''.$$

Proof The proof is by induction on the degree of α. First of all, suppose that $\alpha \in V^*$, i.e., $\deg(\alpha) = 1$. Write $S = \mathbb{F}[t_1, \dots, t_n]$. It suffices to verify the formula for any monomial $t^E = t_1^{e_1} \cdots t_n^{e_n}$. By property (E-2), we have $D_\alpha(t_i) = \langle \alpha, t_i \rangle$. By the derivation property of D_α, we then have

$$D_\alpha(t^E) = \sum_i e_i t^{E_i} \langle \alpha, t_i \rangle, \quad \text{where } E_i = (e_1, e_2, \dots, e_{i-1}, e_{i+1}, \dots, e_n).$$

A direct analogy of a previous result for Δ^* is that the coproduct $\Delta\colon S \to S \otimes S$ satisfies

$$\Delta(t^E) = \sum_{F+G=E} (F, G) t^F \otimes t^G,$$

where

$$(F, G) = \frac{E!}{F!\, G!}.$$

We can reformulate the above identity as

$$D_\alpha(t^E) = \sum_{F+G=E} (F, G) \langle \alpha, t^F \rangle t^G,$$

which is the desired formula.

Next, pick $k \geq 2$ and suppose that the lemma holds in degree $< k$. In proving the lemma in degree k, we can reduce to monomials. Every monomial α of degree k can be decomposed $\alpha = \alpha'\alpha''$, where $\deg(\alpha')$, $\deg(\alpha'') < k$. In particular, the lemma holds for $D_{\alpha'}$ and $D_{\alpha''}$. Pick $x \in S$ and write $\Delta(x) = \sum_i x_i' \otimes x_i''$. Since $(\Delta \otimes 1)\Delta = (1 \otimes \Delta)\Delta$, we can write

$$(\Delta \otimes 1)\Delta(x) = (1 \otimes \Delta)\Delta(x) = \sum_i x_i' \otimes x_{ij} \otimes x_i''$$

where x_i' and x_i'' are as above. We now have the identities

$$D_\alpha(x) = D_{\alpha'}D_{\alpha''}(x) = D_{\alpha'}\Big[\sum_i \langle \alpha'', x_i'\rangle x_i''\Big] = \sum_{i,j} \langle \alpha'', x_i'\rangle \langle \alpha', x_{ij}\rangle x_j''$$

$$= \sum_j \langle \alpha'' \otimes \alpha', \Delta(x_j')\rangle x_j'' = \sum_j \langle \alpha''\alpha', x_j'\rangle x_j''$$

$$= \sum_j \langle \alpha, x_j'\rangle x_j''. \qquad \blacksquare$$

We close this section with a few remarks about the action of S^* on S.

(a) First of all, we explicitly note that, for a constant $c \in \mathbb{F} = S_0^*$, we have

$$D_c(x) = cx \quad \text{for all } x \in S.$$

(b) Next, the action $S^* \otimes S \longrightarrow S$ actually incorporates the pairing $\langle \_, \_\rangle : S^* \otimes S \longrightarrow \mathbb{F}$. More precisely, it follows from Lemma A that

(E-4) for any $\alpha \in S_k^*$ and $x \in S_k$, $D_\alpha(x) = \langle \alpha, x\rangle$.

For we can write $\Delta(x) = x \otimes 1 + \sum_i x_i' \otimes x_i''$, where $\deg(x_i') < k$. So $D_\alpha(x) = \sum_i \langle \alpha, x_i'\rangle x_i''$ reduces to $D_\alpha(x) = \langle \alpha, x\rangle$.

(c) Lastly, we want to observe that it follows from the above lemma that the action $S^* \otimes S \longrightarrow S$ is equivalent, in an appropriate sense, to the product $S^* \otimes S^* \longrightarrow S^*$. The relationship is one of duality and is given by the following lemma.

Lemma B *For any $\alpha, \beta \in S^*$, $x \in S$, $\langle \alpha, D_\beta(x)\rangle = \langle \alpha\beta, x\rangle$.*

Proof $\langle \alpha\beta, x\rangle = \langle \alpha \otimes \beta, \Delta(x)\rangle = \langle \alpha \otimes \beta, \sum_i x_i' \otimes x_i''\rangle = \langle \alpha, \sum x_i' \langle \beta, x_i''\rangle\rangle = \langle \alpha, D_\beta(x)\rangle$. The last equality follows from the previous lemma. $\blacksquare$

25-3 Group actions

As a preparation for the discussion of harmonics in §25-4, we introduce group actions into the map $S^* \otimes S \longrightarrow S$. Given a group $G \subset \mathrm{GL}(V)$, there is a dual action of G on V^* determined by

(F-1) $\langle \varphi \cdot \alpha, x\rangle = \langle \alpha, \varphi^{-1} \cdot x\rangle$ for any $x \in V$, $\alpha \in V^*$ and $\varphi \in G$.

There are induced actions of G on S and S^* and, if we consider the bilinear pairing

$$\langle \_, \_\rangle : S^* \otimes S \longrightarrow \mathbb{F},$$

then the actions are also related as above. In particular, the bilinear pairing is G-equivariant, i.e.,

(F-2) $\langle \varphi \cdot \alpha, \varphi \cdot x \rangle = \langle \alpha, x \rangle$ for $x \in S$, $\alpha \in S^*$ and $\varphi \in G$.

The actions of G on S and S^* are related, in terms of the map $S^* \otimes S \to S$, by:

Lemma $\varphi \cdot D_\alpha(x) = D_{\varphi \cdot \alpha}(\varphi \cdot x)$ *for any* $x \in S$, $\alpha \in S^*$ *and* $\varphi \in G$.

Proof We use the definition of D_α given above in Lemma 25-2A. Suppose $x \in S$ satisfies $\Delta(x) = \sum_i x_i' \otimes x_i''$ and, hence, $\Delta(\varphi \cdot x) = \sum_i \varphi \cdot x_i' \otimes \varphi \cdot x_i''$. Then

$$\begin{aligned} \varphi \cdot D_\alpha(x) &= \sum_i \langle \alpha, x_i' \rangle \varphi \cdot x_i'' \quad \text{(by Lemma 25-2A)} \\ &= \sum_i \langle \varphi \cdot \alpha, \varphi \cdot x_i' \rangle \varphi \cdot x_i'' \quad \text{(by (F-2))} \\ &= D_{\varphi \cdot \alpha}(\varphi \cdot x) \quad \text{(by Lemma 25-2A).} \end{aligned}$$

25-4 Harmonic elements

The invariants of S have been considered in the past few chapters. We can also look at the invariants of S^*. As above, the action of G on V induces an action on V^* and, hence, on S^*. So we can consider $R^* = S^{*G}$. Let

$$R_+^* = \sum_{i \geq 1} R_i^*.$$

The difference between working in R^* and R_+^* is that, in the first case, elements $\alpha \in R^*$ are allowed to have nontrivial constant terms ($= \alpha(0)$).

Definition: $x \in S$ is said to be *harmonic* if $D_\alpha(x) = 0$ for all $\alpha \in R_+^*$, or, equivalently, if $D_\alpha(x) = \alpha(0)x$ for all $\alpha \in R^*$.

Regarding the equivalence of these two conditions, recall that $D_c(x) = cx$ for any constant $c \in \mathbb{F}$. We shall use the following:

Notation: $H =$ the harmonic elements of S.

Remark: The Coxeter groups $W(A_{n-1}) = \Sigma_n$, $W(B_n) = (\mathbb{Z}/2\mathbb{Z})^n \rtimes \Sigma_n$ and $W(D_n) = (\mathbb{Z}/2\mathbb{Z})^{n-1} \rtimes \Sigma_n$ all act by permuting $\{t_1, \ldots, t_n\}$, as well as by changing their signs. It follows that $t_1^2 + \cdots + t_n^2$ is an invariant of each of them. Consequently, a harmonic element in each of these cases must satisfy

$$\Delta(x) = 0,$$

where $\Delta = \frac{\partial^2}{\partial^2 t_1} + \cdots + \frac{\partial^2}{\partial^2 t_n}$ is the usual Laplacian. This equation is the usual definition of a harmonic function.

We remark upon some structural properties of the harmonics $H \subset S$.

(a) First of all, H is an S^* submodule of S. In other words, the action of S^* on S via the maps $D_\alpha\colon S \longrightarrow S$ leaves H stable. For, if $x \in H$, then, for any $\alpha \in S^*$, $\beta \in R^*$,

$$D_\beta D_\alpha(x) = D_\alpha D_\beta(x) = D_\alpha(0) = 0.$$

So $D_\alpha(x) \in H$. This action of S^* on H will be used in the next chapter.

(b) Notice also that H is a G submodule of S. The proof is analogous to that given above for the S^* submodule property.

(c) In analogue to the ideal $I \subset S$ defined in Chapter 18, we can form

$$I^* = \{\beta\alpha \mid \beta \in S^*, \alpha \in R_+^*\} = \text{the ideal of } S^* \text{ generated by } R_+^*.$$

The third property of H concerns the duality existing between the submodule $H \subset S$ and the quotient module $S^* \longrightarrow S^*/I$. It is easily seen that the definition of H can be strengthened to assert that:

Lemma A *$x \in H$ if and only if $D_\alpha(x) = 0$ for all $\alpha \in I^*$.*

This leads to the following duality relationship.

Lemma B *The submodule $H \subset S$ is dual to the quotient module $S^* \longrightarrow S^*/I^*$.*

Proof Pick $\alpha \in S^*, \beta \in R^*$. By Lemma 25-2B we have the identity

$$\langle \alpha\beta, x\rangle = \langle \alpha, D_\beta(x)\rangle \quad \text{for any } x \in S.$$

Moreover ,

$$\langle \alpha, D_\beta(x)\rangle = 0 \quad \text{for all } \alpha \text{ and } \beta \text{ as above if and only if } x \in H.$$

It follows from the above equalities that $H =$ the annihilator of I^* under the nonsingular pairing $\langle \_, \_\rangle$. So there is an induced nonsingular pairing between S^*/I^* and H. ■

Remark: Since S^*/I^* is a quotient algebra, it follows that $H \subset S$ is a sub coalgebra.

This duality between $H \subset S$ and S^*/I^* can be further extended. It is clear, from the above argument, that the action of S^* on H dualizes, in an appropriate manner, to determine the algebra structure of S^*/I^*. These structures will be studied further in Chapter 26. It will be shown that, when G is a pseudo-reflection group, then H is a "cyclic" S^* module, and that this property is equivalent to the algebra H satisfying "Poincaré duality".

26 Harmonics and reflection groups

In this chapter, we use harmonic elements to characterize pseudo-reflection groups over fields of characteristic zero. This characterization is then used to demonstrate that isotropy subgroups of a nonmodular pseudo-reflection group are also pseudo-reflection groups. This fact will play a crucial role in the study of regular elements in Chapter 33. All of the arguments of this section are due to Steinberg [2].

26-1 Main results

As in Chapter 25, *let* $\mathbb{F}$ *be a field of characteristic zero*, V a finite dimensional vector space over $\mathbb{F}$, and $G \subset \mathrm{GL}(V)$ a finite group. We continue to use the notation

$$S = S(V) \quad R = S^G \quad R_+ = \sum_{i\geq 1} R_i \quad I = \text{the ideal } (R_+)$$

$$S^* = S(V^*) \quad R^* = S^{*G} \quad R^*_+ = \sum_{i\geq 1} R^*_i \quad I^* = \text{the ideal } (R^*_+).$$

It was shown in Chapter 18 that $G \subset \mathrm{GL}(V)$ being a pseudo-reflection group is equivalent to either of the following conditions:

(i) R is a polynomial algebra;
(ii) S is a free R module.

In this chapter, we use the harmonics as defined in §25-4 to produce another characterization of pseudo-reflection groups in the characteristic zero case. Recall that in §25-4 we defined the harmonic elements $H \subset S$ by interpreting S^* as a ring of differential operators acting on S, and letting

$$\begin{aligned} H &= \{x \in S \mid D_\alpha(x) = \alpha(0)x \text{ for all } \alpha \in R^*\} \\ &= \{x \in S \mid D_\alpha(x) = 0 \text{ for all } \alpha \in R^*_+\}. \end{aligned}$$

It was also observed in §25-4 that H is a S^* submodule of S. Recall that a S^* module is *cyclic* if it is generated by a single element. In this chapter, we shall prove that:

Theorem **(Steinberg)** *Let V be a finite dimensional vector space over a field $\mathbb{F}$ of characteristic zero, and let $G \subset \mathrm{GL}(V)$ be a finite group. Then G is a pseudo-reflection group if and only if H is a cyclic S^* module.*

We shall actually prove a more detailed result. Let $G \subset \mathrm{GL}(V)$ be a pseudo-reflection group, and let

$$\Omega = \prod_s \alpha_s$$

be the associated skew-invariant element of G defined in §25-2. We shall show that Ω is harmonic and, when H is cyclic, that Ω can be chosen to be the S^* cyclic generator of H.

We remark that this rather technical characterization of pseudo-reflection groups can be reformulated in terms of the property that the algebra H satisfies "Poincaré duality". This equivalence is discussed in §26-7. However, the cyclic module version of the property is the more useful one for the arguments of this chapter. The Steinberg Theorem has important applications. In particular, it can be used to extend a result from §8-1 about the isotropy groups of Euclidean reflection groups.

Definition: Given a set $\Gamma \subset V$, the *isotropy group* of Γ is

$$G_\Gamma = \{\varphi \in G \mid \varphi \cdot x = x \text{ for all } x \in \Gamma\}.$$

We can use this characterization of pseudo-reflection groups to show:

Corollary **(Steinberg)** *Let V be a finite dimensional vector space over a field $\mathbb{F}$ of characteristic zero, and let $G \subset \mathrm{GL}(V)$ be a finite pseudo-reflection group. For any set $\Gamma \subset V$, $G_\Gamma \subset G$ is a pseudo-reflection group.*

This corollary will be used in Chapters 32 and 34 during the study of regular elements.

The arguments of this chapter will involve not only the invariant theory and the skew-invariant theory of S, but also those of S^*. The discussion, in previous chapters, of this theory for S also applies to S^* without any significant alterations. So we freely use the analogous results for S^* in what follows.

26-2 Harmonics of pseudo-reflection groups are cyclic

In this section, we prove one of the implications from Theorem 26-1. Assume that V is a finite dimensional vector space over a field $\mathbb{F}$ of characteristic zero, and that $G \subset \mathrm{GL}(V)$ is a pseudo-reflection group. As in §25-2, form the skew invariant element

$$\Omega = \prod_s \alpha_s$$

in S. This section will be devoted to proving:

Proposition *H is a cyclic S^* module with $\Omega = \prod_s \alpha_s$ as generator.*

First of all, we have:

Lemma A *Ω is harmonic.*

Proof Given $\alpha \in R^*$ of degree > 0, we want to show that $D_\alpha(\Omega) = 0$. For any $\varphi \in G$,

$$\varphi \cdot D_\alpha(\Omega) = D_{\varphi\cdot\alpha}(\varphi \cdot \Omega) = D_\alpha[(\det\varphi)^{-1}\Omega] = \det(\varphi)^{-1} D_\alpha(\Omega).$$

So $D_\alpha(\Omega)$ is a skew invariant. By Proposition 20-2B, $D_\alpha(\Omega)$ is divisible by Ω. But $\deg D_\alpha(\Omega) < \deg \Omega$. Thus $D_\alpha(\Omega) = 0$. ∎

Next, let

$$H(\Omega) = \{D_\alpha(\Omega) \mid \alpha \in S^*\}.$$

Since $\Omega \in H$, and since H is invariant under the action of S^* on S, we have

$$H(\Omega) \subset H.$$

The proposition asserts that this inclusion is an equality. It clearly suffices to prove $\dim_{\mathbb{F}} H \leq \dim_{\mathbb{F}} H(\Omega)$. Let

$$I^* = \text{the ideal of } S^* \text{ generated by } R_+^* = \sum_{i \geq 1} R_+^i.$$

The ideal I^* and the quotient algebra S^*/I^* were considered in §25-4. We shall show that

$$\dim_{\mathbb{F}} H = \dim_{\mathbb{F}} S^*/I^* \leq \dim_{\mathbb{F}} H(\Omega).$$

The first equality follows from Lemma 25-4B, where it was established that the submodule $H \subset S$ is the dual of the quotient $S^* \longrightarrow S^*/I^*$. The second inequality will follow from:

Lemma B *Given $\alpha \in S^*$ of degree > 0, then $D_\alpha(\Omega) = 0$ if and only if $\alpha \in I^*$.*

This lemma implies that the action of S^* on $H(\Omega)$ induces a faithful action of S^*/I^* on Ω.

Proof of Lemma B First of all, Lemma A easily extends to assert that $D_\alpha(\Omega) = 0$ for all $\alpha \in I^*$, since we can write

$$I^* = \{\beta\alpha \mid \beta \in S^*, \alpha \in R_+^*\}$$

and, given $\beta \in S^*$ and $\alpha \in R_+^*$, then $D_{\beta\alpha}(\Omega) = D_\beta D_\alpha(\Omega) = 0$. So the proof of the proposition consists of showing the reverse implication, namely that

$$(*) \qquad D_\alpha(\Omega) = 0 \text{ implies } \alpha \in I^*.$$

We prove statement $(*)$ by downward induction on $\deg\alpha$. Since S^*/I^* is finite dimensional, we know that $\alpha \in I^*$ when α has high degree. So pick $\alpha \in I^*$ and assume that $(*)$ is true in degree $> \deg\alpha$. First of all, we can use this induction hypothesis to show that

(a) $(\det\varphi)\varphi \cdot \alpha \equiv \alpha \pmod{I^*}$

for every $\varphi \in G$. Here $\det\colon G \longrightarrow \mathbb{F}$ is induced by the embedding $G \subset \mathrm{GL}(V^*)$. Since det is multiplicative, and G is generated by pseudo-reflections, we can reduce the proof of (a) to the case where $\varphi = s$, a pseudo-reflection. Choose $\gamma \in V^* \subset S^*$ so that $s\colon V^* \longrightarrow V^*$ satisfies

$$s \cdot \gamma = (\det s)\gamma.$$

Now, $D_{\gamma\alpha}(\Omega) = D_\gamma D_\alpha(\Omega) = 0$. So, by the induction hypothesis, $\gamma\alpha \in I^*$. Write

$$R^* = \mathbb{F}[\omega_1, \ldots, \omega_n].$$

Hence, $I^* = S^*\omega_1 + \cdots + S^*\omega_n$ and we can expand

$$\gamma\alpha = \lambda_1\omega_1 + \cdots + \lambda_n\omega_n,$$

where $\lambda_i \in S^*$. We have

$$(\det s)\gamma(s \cdot \alpha) = (s \cdot \gamma)(s \cdot \alpha) = s \cdot (\gamma\alpha) = (s \cdot \lambda_1)\omega_1 + \cdots + (s \cdot \lambda_n)\omega_n.$$

Since $s \cdot \alpha_i = \alpha_i + \Delta(\lambda_i)\gamma$, we have

$$(s \cdot \lambda_i - \lambda_i)/\gamma = \Delta(\lambda_i).$$

By combining these last three relations, we can write

$$\begin{aligned}(\det s)(s \cdot \alpha) - \alpha &= [(s \cdot \lambda_1 - \lambda_1)/\gamma]\omega_1 + \cdots + [(s \cdot \lambda_n - \lambda_n)/\gamma]\omega_n \\ &= \Delta(\lambda_1)\omega_1 + \cdots + \Delta(\lambda_n)\omega_n.\end{aligned}$$

Thus $(\det s)(s \cdot \alpha) - \alpha \in I^*$ and (a) is proved.

Let Ω^* be the analogue in S^* of the skew-invariant element Ω in S. We next reduce to the case where

(b) $\alpha \equiv \lambda\Omega^* \pmod{I^*}$ for some $\lambda \in \mathbb{F}$.

We have equation (a) for each $\varphi \in G$. Add the left-hand side of all these equations together and then divide by $|G|$. Do the same for the right-hand side. We then obtain the relation

$$\mathrm{Sk}(\alpha) \equiv \alpha \pmod{I^*},$$

where $\mathrm{Sk}\colon S^* \to S^*$ is the projection map for the skew invariants of S^* defined by

$$\mathrm{Sk}(x) = \frac{1}{|G|}\sum_{\varphi\in G}(\det\varphi)\varphi \cdot x.$$

By Proposition 25-2B

$$\alpha \equiv \beta\Omega^* \pmod{I^*},$$

where $\beta \in R^*$. If $\deg\beta > 0$, then $\alpha \in I^*$ and we are done. So we are reduced to β being a constant. We have

(c) $\langle\Omega^*, \Omega\rangle \neq 0$.

For, by Lemma 24-4B,

$$S_N^* = \mathbb{F}\Omega^* \oplus I_N^*.$$

And, by property (E-4) in §25-3, we have

$$\langle \gamma, \Omega \rangle = D_\gamma(\Omega) = 0 \quad \text{for all } \gamma \in I_N^*.$$

The nonsingularity of the pairing $\langle \_, \_ \rangle$ then forces $\langle \Omega^*, \Omega \rangle \neq 0$.

On the other hand, the hypothesis that $D_\alpha(\Omega) = 0$ forces

(d) $\langle \alpha, \Omega \rangle = 0$.

We need only consider α having the same degree as Ω to see this. And, again using property (E-4) of §25-3, we have $\langle \alpha, \Omega \rangle = D_\alpha(\Omega) = 0$.

Finally, by comparing (c) and (d), we have $\lambda = 0$ in (b). So $\alpha \equiv 0 \bmod I^*$. ■

26-3 Generalized harmonics

This section is a preliminary to the arguments of §26-4, §26-5 and §26-6. It introduces a generalization of the harmonics $H \subset S$ and studies some of its properties. For the rest of this chapter, we pass from the polynomials $S = S(V)$ and work with the formal power series $S((V))$. Actually, it suffices (and is convenient) to work with a subalgebra $\widehat{S} \subset S((V))$. For each $x \in V \subset S$, we have

$$e^x = \sum_{n=0}^{\infty} x^n/n!$$

in $S((V))$. Let

$$\widehat{S} = \text{the subalgebra of } S((V)) \text{ generated by } S \text{ and } \{e^x \mid x \in V\}.$$

The differential action of S^* on S extends to an action of S^* on $\widehat{S}$. Just differentiate e^x in the usual manner. In other words, for any $\alpha \in S^*$, we have

$$D_\alpha(e^x) = \alpha(x)e^x.$$

Here *we are interpreting the elements of S^* as polynomial functions on V so that $\alpha(x)$ denotes the value of the polynomial $\alpha \in S^*$ on $x \in V$*. For each $x \in V$, we can define an analogue of the harmonic polynomials.

Definition: $H_x = \{y \in \widehat{S} \mid D_\alpha(y) = \alpha(x)y \text{ for all } \alpha \in R^*\}$.

We shall need the following properties of H_x.

(a) Each H_x is a S^* submodule of $\widehat{S}$.

Pick $\alpha \in R^*$, $\beta \in S^*$ and $y \in H_x$. Then

$$D_\alpha D_\beta(y) = D_\beta D_\alpha(y) = \alpha(x)D_\beta(y).$$

So $D_\beta(y) \in H_x$.

(b) Each H_x is a G submodule of $\widehat{S}$.

Pick $\alpha \in R^*$, $y \in H_x$ and $\varphi \in G$. Then

$$D_\alpha(\varphi \cdot y) = \varphi \cdot D_{\varphi^{-1}\cdot\alpha}(y) = \varphi \cdot D_\alpha(y) = \alpha(x)\varphi \cdot y.$$

So $\varphi \cdot y \in H_x$.

The Automorphism ϕ_x We now introduce notation to help us better describe the action of S^* on each H_x. For each $x \in V$ we can define an automorphism

$$\phi_x \colon S^* \to S^*$$

by the rules that

$$\phi_x(\alpha) = \alpha + \alpha(x) \quad \text{for each } \alpha \in V^*$$
$$\phi_x(\alpha\beta) = \phi_x(\alpha)\phi_x(\beta) \quad \text{for each } \alpha, \beta \in S^*.$$

Observe that, for any $\alpha \in S^*$, we have

(G-1) $\phi_x(\alpha)(0) = \alpha(x)$.

The map ϕ_x is related to the action of G on S and S^* by the formula

(G-2) $\varphi \cdot \phi_x(\alpha) = \phi_{\varphi\cdot x}(\varphi \cdot \alpha)$

for any $x \in S$, $\alpha \in S^*$ and $\varphi \in G$. So ϕ_x is not G-equivariant but, if we let

$$G_x = \text{the isotropy group of } x \in V,$$

then ϕ_x is G_x-equivariant, i.e., $\varphi \cdot \phi_x(\alpha) = \phi_x(\varphi \cdot \alpha)$ for all $\varphi \in G_x$. So ϕ_x restricts to give an isomorphism

$$\phi_x \colon (S^*)^{G_x} \cong (S^*)^{G_x}.$$

Our next formula is, essentially, the motivation for introducing the automorphism ϕ_x. For any $\alpha \in S^*$ and $y \in \widehat{S}$, we have the relation

(G-3) $D_\alpha(e^x y) = e^x D_{\phi_x(\alpha)}(y)$.

It suffices to verify (G-3) for the elements $\alpha \in V^*$ generating S^*. It has already been observed in Chapter 25 that, for $\alpha \in V^*$, the operator D_α is a derivation. Hence,

$$\begin{aligned} D_\alpha(e^x y) &= D_\alpha(e^x)y + e^x D_\alpha(y) = \alpha(x)e^x y + e^x D_\alpha(y) \\ &= e^x[D_{\alpha(x)}(y) + D_\alpha(y)] = e^x D_{\alpha+\alpha(x)}(y), \end{aligned}$$

which is identity (G-3) for $\alpha \in V^*$.

As the first application of the above automorphisms we locate, for each $x \in V$, certain canonical elements of H_x. We clearly have $e^x \in H_x$. More generally, we have

$$e^{\varphi \cdot x} \in H_x \quad \text{for each } \varphi \in G.$$

For, given $\alpha \in R^*$, we have

$$D_\alpha(e^{\varphi \cdot x}) = \alpha(\varphi \cdot x)e^{\varphi \cdot x} = \alpha(x)e^{\varphi \cdot x}.$$

The last equality is based on the fact that $\alpha \in R^*$ and, so, $\alpha(\varphi \cdot x) = \varphi^{-1}\alpha(x) = \alpha(x)$. We can expand this collection of elements in H_x by using the subspace $H^{(x)} \subset H$

$$\begin{aligned} H^{(x)} &= \text{the harmonic elements with respect to } G_x \\ &= \{y \in S \mid D_\alpha(y) = 0 \text{ for all } \alpha \in (S^*)^{G_x}\}. \end{aligned}$$

It is not true that $H^{(x)} \subset H_x$. Rather, the following holds.

Lemma A $e^x H^{(x)} \subset H_x$.

Proof Pick $\alpha \in R^*$ and $h \in H^{(x)}$. Then, by identity (G-2) above,

$$D_\alpha(e^x h) = e^x D_{\phi_x(\alpha)}(h).$$

By the discussion following identity (G-2), $\phi_x(\alpha) \in (S^*)^{G_x}$. So, by the definition of $H^{(x)}$ and identity (G-1),

$$D_{\phi_x(\alpha)}(h) = \phi_x(\alpha)(0)h = \alpha(x)h.$$

Thus

$$D_\alpha(e^x h) = \alpha(x)e^x h.$$

■

The argument used to prove Lemma A shows, more generally, that:

Lemma B $e^{\varphi \cdot x}H^{(x)} \subset H_x$ *for any* $\varphi \in G$.

Proof For any $\alpha \in R^*$, we have the identities

$$D_\alpha(e^{\varphi \cdot x}h) = e^{\varphi \cdot x}D_{\phi_{\varphi \cdot \alpha}}(h)$$

$$D_{\phi_{\varphi \cdot x}(\alpha)}(h) = \alpha(\varphi \cdot x)h = \alpha(x)h.$$

The last equality is based on $\alpha \in R^*$ and, so, $\alpha(\varphi \cdot x) = \varphi^{-1}\alpha(x) = \alpha(x)$. Combining the above two identities, we have

$$D_\alpha(e^{\varphi \cdot x}h) = \alpha(x)e^{\varphi \cdot x}h.$$

■

26-4 Cyclic harmonics

This section is another preliminary section before we complete (in §26-5) the proof of Theorem 26-1 and then prove (in §26-6) Corollary 26-1. In this section, we assume that the harmonics H are a cyclic S^* module, and demonstrate that the cyclic generator P of H can be chosen to satisfy special properties. We then use these properties to define a canonical element P_x of the generalized harmonics H_x for each $x \in V$. We shall define P_x in this section and prove:

Proposition A *If H is a cyclic S^* module, then, for all $x \in V$, H_x is also a cyclic S^* module generated by P_x.*

By considering the action of S^* on P_x, we can also show:

Proposition B *If H is a cyclic S^* module, then, for all $x \in V$,* $\dim_{\mathbb{F}} H_x \geq \dim_{\mathbb{F}} S^*/I^*$.

We shall proceed by first studying the cyclic generator $P \in H$, then defining the element $P_x \in H_x$ and, finally, studying the relation between P_x and P.

Proposition B will be used in §26-5, whereas Proposition A will not be used until §26-6.

(a) The Cyclic Generator P We first show that P can be chosen to satisfy:

Lemma A *P is homogeneous.*

Proof If we decompose P as a sum of its homogeneous components

$$P = P_r + P_{r+1} + P_{r+2} + \cdots + P_m,$$

then $P_k \in H$ for each k. To see this, pick a homogeneous element $\alpha \in R_+^*$. If the resulting equation $D_\alpha(P) = 0$ is decomposed into its homogeneous components, then we obtain the homogeneous equations $D_\alpha(P_k) = 0$.

Suppose P_m is the nonzero component of P of highest degree. Since $P_m \in H$, and P is the cyclic generator of H, we can choose $\beta \in S^*$ such that

$$P_m = D_\beta(P).$$

We also have

$$\beta(0) = 1.$$

For, by definition, when we apply D_β to $P = P_r + P_{r+1} + P_{r+2} + \cdots + P_m$ we obtain $D_\beta(P) = \beta(0)P_m +$ terms of lower degree. Compare this with the previous identity $D_\beta(P) = P_m$.

Since P generates H, and since $D_\beta(P) \in H$, it follows that D_β maps H to H. It follows from the property $\beta(0) = 1$ that the map

$$D_\beta \colon H \to H$$
$$\alpha \mapsto D_\beta(\alpha)$$

is an isomorphism of S^* modules. For given any homogeneous element $\alpha \in H$, we have

$$D_\beta(\alpha) = \beta(0)\alpha + \text{terms of lower degree}$$
$$= \alpha + \text{terms of lower degree.}$$

In particular, since D_β maps P to P_m, it follows that P_m is also a cyclic generator of H. ■

In what follows, assume that P is a homogeneous generator of H.

Lemma B *$\varphi \cdot P = \epsilon(\varphi)P$ for some group homomorphism $\epsilon\colon G \to \mathbb{F}^*$.*

Proof We observed in §25-4 that $H \subset S$ is a G submodule. Hence, for every $\varphi \in G$, we have $\varphi \cdot P \in H$ and, so,

$$\varphi \cdot P = D_\beta(P)$$

for some $\beta \in S^*$. By arguing as in the proof of Proposition A, we have $\beta(0) \neq 0$. It is easy to see that the map

$$\epsilon\colon G \to \mathbb{F}^*$$
$$\epsilon(\varphi) = \beta(0)$$

is multiplicative. ■

Lemma C *P is a homogeneous element of minimal degree in S satisfying the rule $\varphi \cdot x = \epsilon(\varphi)x$ for all $\varphi \in G$. It is unique up to scalar multiple.*

Proof Suppose Q is homogeneous and has minimal degree with respect to elements satisfying the condition $\varphi \cdot x = \epsilon(\varphi)x$ for all $\varphi \in G$. Given $\alpha \in R^*_+$, then the minimal degree condition forces $D_\alpha(Q) = 0$. So $Q \in H$ and

$$Q = D_\beta(P) \quad \text{for some } \beta \in S^*.$$

Fixing β, we can then extend this identity to

$$Q = D_{\varphi\cdot\beta}(P) \quad \text{for each } \varphi \in G.$$

For

$$D_{\varphi\cdot\beta}(P) = \varphi \cdot D_\beta(\varphi^{-1} \cdot P) = \varphi \cdot [\epsilon(\varphi)^{-1} D_\beta(P)]$$
$$= \epsilon(\varphi)^{-1}\varphi \cdot Q = \epsilon(\varphi)^{-1}\epsilon(\varphi)Q = Q.$$

By averaging the above equation, we obtain

$$Q = \frac{1}{|G|}\sum_{\varphi\in G} D_{\varphi\cdot\beta}(P) = D_\gamma(P) \quad \text{where } \gamma = \frac{1}{|G|}\sum_{\varphi\in G} \varphi\cdot\beta = \mathrm{Av}(\beta).$$

However, $\gamma = \mathrm{Av}(\beta) \in R^*$. So $P \in H$ forces $D_\gamma(P) = \gamma(0)P$. Hence, $Q = \gamma(0)P$. ■

(b) The Element P_x Next, let $\epsilon\colon G \to \mathbb{F}^*$ be the group homomorphism determined above. We can define a canonical element $P_x \in H_x$ associated with ϵ. First of all, let

$$\begin{aligned} P^{(x)} = {} & \text{a homogenous element from } S \text{ of minimal degree} \\ & \text{satisfying } \varphi \cdot y = \epsilon(\varphi)y \text{ for all } \varphi \in G_x. \end{aligned}$$

Lemma D $P^{(x)} \in H^{(x)}$.

Proof Given $\alpha \in (S^*)^{G_x}$ and $\varphi \in G_x$, we have

$$\varphi \cdot D_\alpha(P^{(x)}) = D_{\varphi\cdot\alpha}(\varphi \cdot P^{(x)}) = D_\alpha\big(\epsilon(\varphi)P^{(x)}\big) = \epsilon(\varphi)D_\alpha(P^{(x)}).$$

By our choice of $P^{(x)}$ as being a homogeneous element of minimal degree, which is an ϵ invariant with respect to G_x, we have $D_\alpha(P^{(x)}) = 0$. ■

Now form the element

$$P_x = \frac{1}{|G|}\sum_{\varphi\in G} \epsilon(\varphi)^{-1}\varphi \cdot (e^x P^{(x)}).$$

Since H_x is invariant under G, it follows from Lemma 26-3A that:

Lemma E $P_x \in H_x$.

Moreover, P_x is an ϵ invariant, i.e.:

Lemma F $\varphi \cdot P_x = \epsilon(\varphi)P_x$ *for all* $\varphi \in G$.

The argument for this property is analogous to that given at the end of §25-1 demonstrating that $\varphi \cdot \mathrm{Sk}(x) = (\det\varphi)^{-1}\,\mathrm{Sk}(x)$ for all $\varphi \in G$.

Lemma G $P_x = cP+$ *higher terms, where* $c \neq 0$.

Proof Since $\varphi \cdot P_x = \epsilon(\varphi)P_x$ for all $\varphi \in G$, it follows from Lemma C and Lemma F that $P_x = cP+$ higher terms. We are left with proving that $c \neq 0$.

We first prove two facts about homogeneous decompositions of elements of h_x. Consider $h \in H_x$ and decompose h into homogeneous pieces

$$h = h_r + h_{r+1} + \cdots \quad (h_r \neq 0),$$

where $h_i \in S_i$. First of all, we have

$$(*) \qquad\qquad h_r \in H.$$

For, given $\alpha \in R^*$, then $D_\alpha(h) = \alpha(x)h$. We can decompose this equation into equations between corresponding homogeneous terms. In particular, $D_\alpha(h_r) = 0$. Secondly, we have

$$(**) \qquad r > \deg P \text{ implies } h = 0.$$

For $h_r \in H$ implies $h_r = D_\alpha(P)$ for some $\alpha \subset S^*$. In particular $\deg h_r \leq \deg P$.

If we apply $(**)$ to the case $h = P_x = cP+$ higher terms, then it follows that $c \neq 0$. ∎

Proof of Proposition A Given $h \in H_x$, it has a decomposition into homogeneous pieces

$$h = h_r + h_{r+1} + \cdots \quad (h_r \neq 0),$$

where $h_i \in S_i$. We shall prove by downward induction on r that h belongs to the cyclic S^* module generated by P_x. For $r > \deg P$, we can use $(**)$. Next, consider general r. Since $h_r = D_\alpha(P)$ for some $\alpha \in S^*$, it follows that $h - c^{-1}D_\alpha(P_x)$ has a decomposition

$$h - c^{-1}D_\alpha(P_x) = \overline{h}_{r+1} + \overline{h}_{r+2} + \cdots .$$

By induction, $h - c^{-1}D_\alpha(P_x)$ belongs to the cyclic S module generated by P_x. Consequently, h does as well. ∎

Proof of Proposition B We shall consider the action of S^* on the element $P_x \in H_x$. We know that $D_\alpha(P_x) \in H_x$ for all $\alpha \in S^*$. The proof of the proposition will consist of showing that, if $\alpha \neq 0$ in S^*/I, then $D_\alpha(P_x) \neq 0$. Let β be the homogeneous part of α of highest degree. In particular, $\beta \neq 0$ in S^*/I^*. Suppose $D_\beta(P_x) = 0$. We shall show that this assumption forces $\beta = 0$ in S^*/I^*, a contradiction.

First of all, the assumption forces

$$(*) \qquad D_\beta(P) = 0.$$

For P is homogeneous and, as already shown in the proof of Proposition A,

$$P_x = cP + \text{higher terms} \quad \text{where } c \neq 0.$$

If we let

$$\ell = \deg P \quad \text{and} \quad m = \deg \beta,$$

then the homogeneous part of $D_\alpha(P_x)$ of degree $\ell - m$ is $D_\beta(P)$. So $D_\alpha(P_x) = 0$ forces $D_\beta(P) = 0$.

Secondly, we can use $(*)$ to force

$$(**) \qquad D_\beta(h) = 0 \quad \text{for all } h \in H.$$

For, by assumption, H is a cyclic S^* module generated by P.

Finally, $(**)$ forces

$$(***) \qquad \langle \beta, h \rangle = 0 \quad \text{for all } h \in H.$$

Assume that h is homogeneous. If degree $\beta \neq$ degree h, there is nothing to prove. If $\deg \beta = \deg h$, then, by property (E-4) of §25-2, we have $\langle \beta, h \rangle = D_\beta(h)$.

By Lemma 25-4B, the submodule $H \subset S$ and the quotient S^*/I^* are dual under the nonsingular pairing $\langle \_, \_ \rangle$. So $(***)$ forces $\beta = 0$ in S^*/I^*, the desired contradiction. ■

26-5 Pseudo-reflection groups are characterized via harmonics

In this section, we prove the other implication of Theorem 26-1:

Proposition *If H is a cyclic S module, then G is a pseudo-reflection group.*

It follows from Theorem 22-5, with Theorem 23-1, that

$$\dim_{\mathbb{F}} S^*/I^* \geq |G|$$

$$\dim_{\mathbb{F}} S^*/I^* = |G| \quad \text{if and only if } G \subset \mathrm{GL}(V^*) \text{ is a pseudo-reflection group.}$$

So to prove the proposition, it suffices to prove that H being a cyclic S^* module forces $\dim_{\mathbb{F}} S^*/I^* = |G|$. Let

$$d_x = \dim_{\mathbb{F}} H_x.$$

Proposition 26-4B demonstrated that $d_x \geq \dim_{\mathbb{F}} S^*/I^*$ for all $x \in V$, provided H is cyclic. We can also prove

$(*)$ If the isotropy group G_x for $x \in V$ is trivial, then $d_x \leq |G|$.

Putting together these facts we have, for the appropriate x,

$$|G| \leq \dim_{\mathbb{F}} S^*/I^* \leq d_x \leq |G|.$$

Thus $\dim_{\mathbb{F}} S^*/I^* = |G|$ as desired.

The rest of this section will be devoted to proving $(*)$. We begin by verifying that there actually exist $x \in V$ for which the isotropy group G_x is trivial. For each $\varphi \in G$, the subspace V^φ of fixed points is a proper subspace. It follows from Lemma 3-3A that $\bigcup_{\varphi \in G} V^\varphi \neq V$.

Assume that $G_x = \{1\}$. We shall show that H_x has an $\mathbb{F}$ basis indexed by elements of G. This will imply that $d_x \leq |G|$. Now, $\widehat{S}$ is spanned by elements of the form $\{e^x P\}$, where $x \in V$ and $P \in S$. So we can expand any $h \in H_x$ as a finite sum

$$h = \sum_i e^{x_i} P_i.$$

We shall show that, for each i,

(a) $e^{x_i}P_i \in H_x$;
(b) P_i is a constant and $x_i = \varphi \cdot x$ for some $\varphi \in G$.

This will complete the proof that $d_x \leq |G|$, since we shall have demonstrated that $\{e^{\varphi \cdot x}\}_{\varphi \in G}$ spans H_x.

Fact (a) is fairly easy to establish. Pick $\alpha \in R^*$. By identity (G-2) of §26-3, we have

$$D_\alpha(e^{x_i}P_i) = e^{x_i}D_{\phi_x(\alpha)}(P_i).$$

The elements $\{e^{x_i}\}$ are linearly independent over S. Consequently, the identity $D_\alpha(h) = \alpha(x)h$, with the above identity, forces

$$D_\alpha(e^{x_i}P_i) = \alpha(x)e^{x_i}P_i \quad \text{for each } i.$$

So $e^{x_i}P_i$ belongs to H_x.

The proof of fact (b) is longer and needs to be broken down into a number of steps.

Lemma A *If $h \in H_x$, then $D_\beta(h) = 0$ for each $\beta = \prod_{\varphi \in G}[\alpha - \langle \varphi \cdot \alpha, x\rangle]$ where $\alpha \in V^*$.*

Proof We have

$$0 = \prod_{\varphi \in G}(\alpha - \varphi \cdot \alpha) = \alpha^k + \epsilon_{k-1}\alpha^{k-1} + \cdots + \epsilon_1\alpha + \epsilon_0,$$

where each ϵ_i is a symmetric polynomial in $\{\varphi \cdot \alpha\}$. In particular, $\epsilon_i \in R^*$. Observe, also, that

$$\beta = \alpha^k + \epsilon_{k-1}(x)\alpha^{k-1} + \cdots + \epsilon_1(x)\alpha + \epsilon_0(x).$$

Consequently, we have

$$\begin{aligned} 0 = D_0(h) &= [D_\alpha^k + D_{\epsilon_{k-1}}D_\alpha^{k-1} + \cdots + D_{\epsilon_1}D_\alpha + D_{\epsilon_0}](h) \\ &= \left[D_\alpha^k + \epsilon_{k-1}(x)D_\alpha^{k-1} + \cdots + \epsilon_1(x)D_\alpha + \epsilon_0(x)\right](h) \\ &= D_\beta(h). \end{aligned}$$

We can use Lemma A to deduce

Lemma B *$D_\alpha^r(P_i) = 0$ for all $\alpha \in V^*$, where $r =$ the number of $\varphi \in G$ where $\varphi \cdot x = x_i$.*

Proof We can apply Lemma A to the element $h = e^{x_i}P_i \in H_x$. Using the identity (G-2) of §26-3, we obtain

$$(*) \qquad e^{x_i}D_{\phi_{x_i}(\beta)}(P_i) = D_\beta(e^{x_i}P_i) = 0,$$

where

$$\beta = \prod_{\varphi \in G} [\alpha - \langle \varphi \cdot \alpha, \cdot x \rangle]$$

$$\phi_{x_i}(\beta) = \prod_{\varphi \in G} [\alpha - \langle \varphi \cdot \alpha, x \rangle + \langle \alpha, x_i \rangle].$$

Equation $(*)$ can clearly be simplified to

$$(**) \qquad D_{\phi_{x_i}(\beta)}(P_i) = 0.$$

Regard $\phi_{x_i}(\beta)$ as a polynomial $f(\alpha)$ in α. Then $D_{\phi_{x_i}(\beta)}$ is the polynomial $f(D_\alpha)$ in D_α. Suppose that we can factor

$$f(\alpha) = g(\alpha)\alpha^k, \quad \text{where } g(0) \neq 0.$$

Then $(**)$ can be rewritten $g(D_\alpha)D_\alpha^k(P_i) = 0$. And $g(0) \neq 0$ forces

$$(***) \qquad D_\alpha^k(P_i) = 0.$$

We want to choose k such that α^k appears as a factor in the above decomposition of $\phi_{x_i}(\beta)$ for every choice of α. Since $\phi_{x_i}(\beta) = \prod_{\varphi \in G}[\alpha - \langle \varphi \cdot \alpha, x \rangle + \langle \alpha, x_i \rangle]$, we want to know how many times

$$-\langle \varphi \cdot \alpha, x \rangle + \langle \alpha, x_i \rangle = 0$$

for every choice of α. This amounts to determining how many $\varphi \in G$ satisfy $x_i = \varphi^{-1} \cdot x$. For we have

$$\begin{aligned} -\langle \varphi \cdot \alpha, x \rangle + \langle \alpha, x_i \rangle &= -\langle \alpha, \varphi^{-1} \cdot x \rangle + \langle \alpha, x_i \rangle \\ &= \langle \alpha, x_i - \varphi^{-1} \cdot x \rangle. \end{aligned}$$

If $\varphi^{-1} \cdot x \neq x_i$, then we can find $\alpha \in V^*$ such that $\langle \alpha, x_i - \varphi^{-1} \cdot x \rangle \neq 0$. ■

Since $G_x = \{1\}$, the only possibilities for r in Lemma B are $r = 0$ or $r = 1$.

Case $r = 0$ This is the case $P_i = 0$, so it can be ignored.

Case $r = 1$ Here $x_i = \varphi \cdot x$ for a unique $\varphi \in G$. Also, the equation $D_\alpha^r(P_i) = 0$ becomes

$$D_\alpha(P_i) = 0 \quad \text{for all } \alpha \in V^*.$$

Since this equation is satisfied for all $\alpha \in V^*$, it follows that P_i is a constant.

26-6 Isotropy subgroups

In this section, we prove Corollary 26-1. First of all, it suffices to prove the corollary for a set consisting of a single element. We can reduce to the case of Γ being finite by using linearity. The reduction to Γ being a single point follows by an inductive argument on $|\Gamma|$. We decompose $\Gamma = \Gamma' \cup \{x\}$ and use the relation $G_\Gamma = (G_{\Gamma'})_x$. So the rest of this section will be devoted to proving:

Proposition *Let V be a finite dimensional vector space over a field $\mathbb{F}$ of characteristic zero, and let $G \subset \mathrm{GL}(V)$ be a finite pseudo-reflection group. Then, for any $x \in V$, G_x is a pseudo-reflection group.*

We shall prove the proposition via our characterization of pseudo-reflection groups in terms of harmonic elements. Because of our hypothesis on G, we know from Theorem 26-1 that the harmonics are a cyclic S^* module. By the arguments of §26-4, we can choose a homogeneous cyclic generator P that transforms according to the rule

$$\varphi \cdot P = \epsilon(\varphi)P$$

for some group homomorphism $\epsilon\colon G \to \mathbb{F}$. Alternatively, we could also take advantage of Proposition 26-2 and simply choose $P = \Omega$ and $\epsilon = \det^{-1}$. However, since we shall want to appeal to the arguments of §26-4, we shall work with P and ϵ, rather than Ω and $\det^{-1}$. As in §26-4, let

$$H^{(x)} = \{y \in S \mid D_\alpha(y) = 0 \text{ for all } \alpha \in (S^*)^{G_x}\}$$

be the harmonic elements with respect to G_x and let

$$P^{(x)} = \text{a homogenous element from } S \text{ of minimal degree satisfying}$$

$$\varphi \cdot y = \epsilon(\varphi)y \quad \text{for all } \varphi \in G_x.$$

We know from §26-4 that $P^{(x)} \in H^{(x)}$. We shall show that $H^{(x)}$ is a cyclic S^* module with $P^{(x)}$ as generator. Theorem 26-1 then implies that G_x is a pseudo-reflection group. In order to show that $P^{(x)}$ generates $H^{(x)}$ as an S^* module, we first pass to $H_x \subset \widehat{S}$. Consider the element

$$P_x = \frac{1}{|G|}\sum_{\varphi \in G_x} \epsilon(\varphi)^{-1}\varphi \cdot (e^x P^{(x)}).$$

We showed in §26-4 that $P_x \in H_x$ and H_x is a cyclic S^* module generated by P_x. We now use this fact to prove:

Lemma *$H^{(x)}$ is a cyclic S^* module generated by $P^{(x)}$.*

Proof Pick $h \in H^{(x)}$. Then, by Lemma 26-3A, $e^x h \in H_x$. So $e^x h = D_\alpha(P_x)$ for some $\alpha \in S^*$. Now,

$$\begin{aligned} e^x h = D_\alpha(P_x) &= \sum_{\varphi \in G_x} \epsilon(\varphi)^{-1} D_\alpha(e^{\varphi \cdot x}\varphi \cdot P^{(x)}) \\ &= \sum_{\varphi \in G_x} \epsilon(\varphi)^{-1} e^{\varphi \cdot x} D_{\phi_{\varphi \cdot x}(\alpha)}(\varphi \cdot P^{(x)}). \end{aligned}$$

The last equality is based on identity (G-3) of §26-2. For any finite set $\{x_1, \ldots, x_k\}$, the elements $\{e^{x_1}, \ldots, e^{x_k}\}$ are linearly independent. Consequently, in the above, we can reduce the last summand to terms involving e^x. In other words, we only consider $\varphi \in G_x$ and obtain

$$e^x h = \sum_{\varphi \in G_x} \epsilon(\varphi)^{-1} e^x D_{\phi_x(\alpha)}(\varphi \cdot P^{(x)}).$$

Since $\varphi \cdot P^{(x)} = \epsilon(\varphi) P^{(x)}$ for all $\varphi \in G_x$, we have

$$e^x h = |G_x| e^x D_{\phi_x(\alpha)}(P^{(x)}).$$

Consequently, $h = |G_x| D_{\phi_x(\alpha)}(P^{(x)})$. ∎

26-7 Poincaré duality

Another important property often possessed by the ring of covariants of pseudoreflection groups is Poincaré duality. As will be explained, this property is equivalent to properties previously studied in this chapter.

Definition: A finite dimensional graded $\mathbb{F}$ algebra A is said to satisfy *Poincaré duality* if there exists a positive integer N such that

(i) $A^N = \mathbb{F}$ while $A^i = 0$ for $i > N$;
(ii) the multiplicative pairing $A^i \otimes A^{N-i} \to A^N = \mathbb{F}$ given by $x \otimes y \mapsto xy$ is nonsingular for each $0 \leq i \leq N$.

The fact that the module of harmonics, $H \subset S$, is a cyclic S^* module can be reformulated in terms of Poincaré duality. Namely, if we use the previous notation of this chapter, then we have:

Proposition *H is a cyclic S^* module if and only if S^*/I^* is a Poincaré duality algebra.*

The action $S^* \otimes H \to H$ induces an action $S^*/I^* \otimes H \to H$. This action is dual to the product map

$$S^*/I^* \otimes S^*/I^* \to S^*/I^*.$$

For, by Lemma 25-2B, along with the duality established between S^*/I^* and H in Lemma 25-4B, we have the identity

$$\langle \alpha\beta, x\rangle = \langle \alpha, D_\beta(x)\rangle \quad \text{for any } \alpha, \beta \in S^*/I^*, x \in H.$$

This identity, along with the duality between H and S^*/I^*, enables us to relate the two conditions appearing above in the statement of the lemma.

First of all, it is easy to see that the Poincaré duality property for S^*/I^* can be reformulated to assert that there exists $\Omega \in H$ such that, for each $\alpha \in S^*/I^*$, there exists $\beta \in S^*/I^*$ such that $\langle \alpha\beta, \Omega\rangle \neq 0$.

Secondly, asserting that H is cyclic with generator Ω is equivalent to asserting that, for every $\alpha \in S^*/I^*$, we can find $\beta \in S^*/I^*$ such that $\langle \alpha, D_\beta(\Omega)\rangle \neq 0$. ∎

VIII Conjugacy classes

In the next four chapters, we return to the earlier topic of Euclidean reflection groups and focus on the conjugacy classes of elements and subgroups in these groups. As in the earlier study of Euclidean reflection groups in Chapters 1 to 8, a theme will be the intimate relation between the algebra of a reflection group and its geometry. The structural theorems obtained will demonstrate significant relations between the conjugacy classes and the underlying root system of a Euclidean reflection group. We might contrast this approach with a second approach to conjugacy classes that uses invariant theory and focuses on the study of eigenvalues and eigenspaces. This other approach is developed in Chapters 31 through 34.

In Chapter 5, we dealt with parabolic subgroups. That chapter can be regarded as a preliminary section for the following four chapters. Parabolic subgroups will play an important role in the study of conjugacy classes.

There is no general, uniform description of the conjugacy classes of elements in a finite Euclidean reflection group. Our discussion will concentrate on two particular classes of elements for which detailed descriptions have been obtained, namely Coxeter elements and involutions. The theoretical classification of involutions carried out by Deodhar, Richardson and Springer is described in Chapter 27. In Chapter 28, we introduce *elementary equivalences* and demonstrate their usefulness in determining the conjugacy classes of parabolic subgroups and of involutions. Coxeter elements are studied in Chapter 29. The main result of Chapter 29 is to relate the order of a Coxeter element to the underlying root system. Aside from reflections, Coxeter elements are probably the most studied elements of Euclidean reflection groups. They will be studied again in Chapters 32 and 34 in the more general context of regular elements. In Chapter 30, we describe Carter's results concerning decompositions of elements of a reflection group into products of reflections.

27 Involutions

The purpose of this chapter is to present a uniform description of the conjugacy classes of involutions in finite reflection groups. As we shall see, involutions are closely related to parabolic subgroups, and the classification of involutions is, in essence, a statement of that relation. The results of this chapter, and of the next, are based on the work of Deodhar [1], Richardson [1] and Springer [4].

Involutions play a key role in reflection groups. For example, it follows from the work of Carter [2] and Springer [2] that every element in a finite reflection group can be written as a product of two involutions. This fact was used by Carter to study arbitrary conjugacy classes in such groups. See Chapter 30 for details.

27-1 Elements of greatest length

Let $W \subset O(\mathbb{E})$ be a reflection group with root system $\Delta \subset \mathbb{E}$. In this section, we use the action of W on Δ to select an important conjugacy class of involutions in W. These involutions, in turn, will be the key to understanding arbitrary involutions.

The W action on Δ enables us to associate a canonical involution $\omega_\Sigma \in W$ to each fundamental system Σ of Δ. Pick a fundamental system $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$. Then $-\Sigma = \{-\alpha_1, \ldots, -\alpha_\ell\}$ is also a fundamental system. The positive roots with respect to Σ are the negative roots with respect to $-\Sigma$, and vice versa. We know from §4-6 that W acts transitively and freely on fundamental systems. So there exists a unique $\omega_\Sigma \in W$ such that

$$\omega_\Sigma \cdot \Sigma = -\Sigma.$$

The element ω_Σ is an involution. For, by linearity, $(\omega_\Sigma)^2 \cdot \Sigma = \Sigma$. The fact that W acts freely on the fundamental systems then forces $(\omega_\Sigma)^2 = 1$.

The element ω_Σ depends on the choice of the fundamental system Σ. However, as the next proposition shows, different choices give rise to conjugate elements.

Proposition *The involutions $\{\omega_\Sigma\}$ associated to the various fundamental systems $\{\Sigma\}$ of Δ form a single conjugacy class in W.*

Proof Pick fundamental systems Σ and Σ' of Δ. Let ω_Σ and ω'_Σ be the elements associated with Σ and Σ'. Since W acts transitively on fundamental systems, there exists $\varphi \in W$ such that $\varphi \cdot \Sigma = \Sigma'$. Then

$$(\varphi\omega_\Sigma\varphi^{-1}) \cdot \Sigma' = (\varphi\omega_\Sigma\varphi^{-1}) \cdot (\varphi \cdot \Sigma) = (\varphi\omega_\Sigma) \cdot \Sigma = -\varphi \cdot \Sigma = -\Sigma'.$$

Since the property $\omega'_\Sigma \cdot \Sigma' = -\Sigma'$ defines ω'_Σ, we must have $\varphi\omega_\Sigma\varphi^{-1} = \omega'_\Sigma$. ■

The property $\omega_\Sigma \cdot \Sigma = -\Sigma$ implies that we can write

$$\omega_\Sigma = -\tau_\Sigma,$$

where τ_Σ is a map permuting the set Σ. Since ω_Σ is an involution, τ_Σ must also be an involution. The involution τ_Σ is most easily understood as a symmetry of

the Coxeter graph of W. To identify τ_Σ with such a symmetry, we regard Σ as the vertices of the Coxeter graph. Below, we look at the cases of the root systems A_ℓ, B_ℓ and D_ℓ.

Examples: In the following, we shall be using the notation of §2-4 and §3-2.

(a) Root System $\Delta = A_\ell$ In this case, $\Delta \subset \mathbb{R}^{\ell+1}$ is the root system given by

$$\Delta = \{\epsilon_i - \epsilon_j \mid i \neq j\},$$

where $\{\epsilon_1, \ldots, \epsilon_{\ell+1}\}$ is an orthonormal basis of $\mathbb{R}^{\ell+1}$. The fundamental roots are

$$\Sigma = \{\alpha_i = \epsilon_i - \epsilon_{i+1} \mid 1 \leq i \leq \ell\}.$$

The action of $W(\Delta) = \Sigma_{\ell+1}$ on Δ is determined by its action on $\{\epsilon_i\}$ as permutations. The involution ω_Σ is the permutation

$$\omega_\Sigma \cdot \epsilon_i = \epsilon_{\ell-i}.$$

So it acts on the fundamental roots Σ by the rule

$$\omega_\Sigma \cdot \alpha_i = -\alpha_{\ell-i}.$$

Thus ω_Σ is the composite of $c = -1$, with the involution τ_Σ being given by $\tau_\Sigma \cdot \alpha_i = \alpha_{\ell-i}$, i.e., τ_Σ is the nontrivial involution of the graph

$$\begin{array}{ccccccc} \circ & - & \circ & - - - & \circ & - & \circ \\ \alpha_1 & & \alpha_2 & & \alpha_{\ell-1} & & \alpha_\ell \end{array}$$

(b) Root System $\Delta = B_\ell$ In this case, $\Delta \subset \mathbb{R}^\ell$ is the root system given by

$$\Delta = \{\pm\epsilon_i\} \coprod \{\pm\epsilon_i \pm \epsilon_j \mid i \neq j\},$$

where $\{\epsilon_1, \ldots, \epsilon_\ell\}$ is an orthonormal basis of $\mathbb{R}^\ell$. The action of $W(\Delta) = (\mathbb{Z}/2\mathbb{Z})^\ell \rtimes \Sigma_\ell$ on Δ is determined by the fact that Σ_ℓ acts on $\{\epsilon_i\}$ as permutations, while $(\mathbb{Z}/2\mathbb{Z})^\ell$ acts on $\{\pm\epsilon_i\}$ as sign changes. In particular, the reflections $\{s_{\epsilon_i}\}$ are the sign changes on the various factors. Additionally,

$$\omega_\Sigma = s_{\epsilon_1} \cdots s_{\epsilon_\ell} = -1.$$

(c) Root System $\Delta = D_\ell$ The root system $\Delta \subset \mathbb{R}^\ell$ is given by

$$\Delta = \{\pm\epsilon_i \pm \epsilon_j \mid i \neq j\},$$

where $\{\epsilon_1, \ldots, \epsilon_\ell\}$ is an orthonormal basis of $\mathbb{R}^\ell$. The fundamental roots are

$$\Sigma = \{\alpha_i = \epsilon_i - \epsilon_{i+1} \mid 1 \leq i \leq \ell - 1\} \coprod \{\alpha_\ell = \epsilon_{\ell-1} + \epsilon_\ell\}.$$

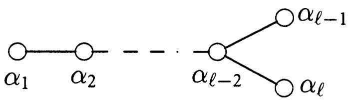
The action of $W(\Delta) = (\mathbb{Z}/2\mathbb{Z})^{\ell-1} \rtimes \Sigma_\ell$ on Δ is determined by the fact that Σ_ℓ acts on $\{\epsilon_i\}$ as permutations, while $(\mathbb{Z}/2\mathbb{Z})^{\ell-1}$ acts on $\{\pm\epsilon_i\}$ as sign changes on an even number of terms. Write $\ell = 2k$ or $\ell = 2k+1$. Then ω_Σ is the map

$$\omega_\Sigma \cdot \epsilon_i = -\epsilon_i \quad \text{for } 1 \leq i \leq 2k.$$

So if $\ell = 2k$, then $\omega_\Sigma = -1$ while, if $\ell = 2k+1$, then ω_Σ is the composite of -1 with the involution τ_Σ that interchanges $\alpha_{\ell-1}$ and α_ℓ, i.e.,

$$\omega \cdot \alpha_i = -\alpha_i \quad \text{for } 1 \leq i \leq \ell - 2$$
$$\omega \cdot \alpha_{\ell-1} = -\alpha_\ell$$
$$\omega \cdot \alpha_\ell = -\alpha_{\ell-1}.$$

In the latter case, ω_Σ differs from $c = -1$ by the nontrivial involution of the graph



This type of analysis can be applied to any reflection group. If we examine the irreducible Coxeter graphs appearing in the classification theorem of §8-1, then, except for D_4, there is only one possible involution of each graph. When τ_Σ is nontrivial, it must be this involution. We can show that the nontrivial cases of τ_Σ (for Δ irreducible) occur when $\Delta = A_k$ $(k \geq 2)$, D_{2k+1}, E_6 and $G_2(2k+1)$. In particular, the cases A_k and D_{2k+1} were demonstrated above.

Additional Properties of ω_Σ We close the section with a few more properties of the elements ω_Σ. The involution ω_Σ satisfies the (equivalent) properties of converting every positive root into a negative root, and of being of maximal length among the elements of W. More exactly, let $\Delta = \Delta^+ \coprod \Delta^-$ be the decomposition of Δ into positive and negative roots with respect to Σ, and let $\ell(\varphi)$ denote the length of elements in W with respect to Σ as defined in §4-4. Then the associated involution ω_Σ satisfies

(H-1) $\omega_\Sigma \cdot \Delta^+ = \Delta^-$;
(H-2) $\ell(\omega_\Sigma) = N$ where $N = |\Delta^+|$.

It follows from the characterization of length in §4-4 that the two properties are equivalent, and that the second can be rephrased as asserting that ω_Σ has maximal length (with respect to Σ) among the elements of W.

We can also show that

(H-3) ω_Σ is the unique element in W of maximal length N (with respect to Σ).

For, if ω'_Σ is also of length N, then $\omega'_\Sigma \cdot \Delta^+ = \Delta^-$. Hence, $(\omega_\Sigma {\omega'_\Sigma}^{-1}) \cdot \Delta^+ = \Delta^+$. Thus $\ell(\omega_\Sigma {\omega'_\Sigma}^{-1}) = 0$ and $\omega_\Sigma {\omega'_\Sigma}^{-1} = 1$.

27-2 The involution $c = -1$

Let $W \subset O(\mathbb{E})$ be a Euclidean reflection group with root system $\Delta \subset \mathbb{E}$, i.e., $W = W(\Delta)$. The close relation between the linear map $c = -1$ and the elements $\{\omega_\Sigma\}$ was discussed in §27-1. In particular, if -1 belongs to $W(\Delta)$, then it satisfies property (H-1) of §27-1 and, so, must be identical to the involution ω_Σ for any fundamental system Σ of Δ. Analyzing ω_Σ on a case-by-case basis, and determining when $\omega_\Sigma = -1$, we can verify that:

Lemma *For an irreducible reflection group $W(\Delta) \subset O(\mathbb{E})$, we have*

(i) $-1 \in W(\Delta)$ *if and only if* $\Delta = A_1, B_k, D_{2k}, E_7, E_8, F_4, G_2(2k), H_3, H_4$;
(ii) $-1 \notin W(\Delta)$ *if and only if* $\Delta = A_k\ (k \geq 2), D_{2k+1}, E_6, G_2(2k+1)$.

More generally, $-1 \in W(\Delta)$ if and only if Δ is a disjoint union (repetitions allowed) of the root systems appearing in part (i) of the lemma. As mentioned before, the cases where $-1 \notin W(\Delta)$ are the cases that $\omega_\Sigma = -\tau_\Sigma$, where τ_Σ permutes the elements of Σ in a nontrivial fashion. The above division of the irreducible root systems will reappear throughout Chapters 27 and 28. In particular, it plays an integral part in the algorithm to be developed for classifying conjugacy classes of involutions. See §28-5 for a discussion of this relation.

It is probably helpful to point out that there is a different approach to this result. The degrees $\{d_1, \ldots, d_\ell\}$ of a reflection group were introduced in §18-1. It will be demonstrated in §31-1 (see Corollary 31-1B) that

$$-1 \in W \quad \text{if and only if all the degrees of } W \text{ are even.}$$

So the above lemma reduces to knowing the degrees of each finite reflection group. Many techniques for determining these degrees will be established in subsequent discussions. This is still a proof by calculation, but perhaps more informed than that involving ω_Σ.

Additional Properties Here are some final comments concerning the element $c = -1$ in the irreducible case.

(i) -1 generates the center of W. In other words, the center of W is either trivial or $\mathbb{Z}/2\mathbb{Z}$ and the $\mathbb{Z}/2\mathbb{Z}$ case occurs precisely when $-1 \in W$;
(ii) If W is essential, then $-1 \in W$ if and only if the root system Δ contains an orthogonal basis of $\mathbb{E}$.

This last fact will be a consequence of Theorem 30-1B.

27-3 The involutions c_I

Let $W \subset O(\mathbb{E})$ be a reflection group with root system $\Delta \subset \mathbb{E}$. Choose a fundamental system $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$ of Δ. The element $c = -1$ from §27-2 can be generalized to a family of involutions $\{c_I\}$ indexed by $I \subset \{1, \ldots, \ell\}$. Moreover,

these involutions will turn out to be the key to classifying arbitrary involutions in a reflection group. For each subset $I \subset \{1, \dots, \ell\}$, let

$$\mathbb{E}^I = \bigcap_{i \in I} H_{\alpha_i} = \{x \in \mathbb{E} \mid (\alpha_i, x) = 0 \text{ for } i \in I\}$$

$$\mathbb{E}_I = \text{the subspace of } \mathbb{E} \text{ generated by } \{\alpha_i \mid i \in I\}.$$

Clearly, we have an orthogonal decomposition $\mathbb{E} = \mathbb{E}^I \oplus \mathbb{E}_I$. Let

$$c_I : \mathbb{E} \to \mathbb{E}$$

denote the involution defined by

$$c_I = \begin{cases} 1 \text{ on } \mathbb{E}^I \\ -1 \text{ on } \mathbb{E}_I. \end{cases}$$

In §27-4, we shall demonstrate that every involution in a reflection group is conjugate to one of the involutions c_I. Consequently, the classification of conjugacy classes of involutions reduces to two questions concerning the involutions $\{c_I\}$.

(Q-1) For which I does $c_I : \mathbb{E} \to \mathbb{E}$ actually belong to $W \subset O(\mathbb{E})$?
(Q-2) Given $c_I \in W$ and $c_J \in W$, when are they conjugate in W?

In the rest of this section, we explain how these questions can be reduced to facts about the root system Δ. Parabolic subgroups and parabolic subroot systems were discussed in Chapter 5. Let

$$\Sigma_I = \{\alpha_i \mid i \in I\}$$

$$\Delta_I = \text{the parabolic subroot system generated by } \Sigma_I$$

$$W_I = \text{the parabolic subgroup generated by } \{s_\alpha \mid \alpha \in \Sigma_I\}.$$

The concept of W equivalence was also introduced in §5-2. The rest of this section will be devoted to proving the following two propositions.

Proposition A *$c_I \in W$ if and only if Δ_I is a disjoint union (repetitions allowed) of A_1, B_k, D_{2k}, E_7, E_8, F_4, $G_2(2k)$, H_3, H_4.*

Proposition B *Given $I, J \subset \{1, \dots, \ell\}$ then the following are equivalent:*

(i) c_I and c_J are conjugate in W;
(ii) W_I and W_J are conjugate in W;
(iii) Δ_I and Δ_J are W-equivalent;
(iv) Σ_I and Σ_J are W-equivalent.

Observe that Proposition B is an extension of Proposition 5-3. We have added condition (i) to the previous set of equivalences. Observe also that the list of root systems appearing in Proposition A is one of the lists appearing in Lemma 27-2. Chapter 28 will be devoted to further analysis of questions (Q-1) and (Q-2). In particular, we shall demonstrate that both questions are most effectively studied by using Coxeter graphs. Propositions A and B play an important role in these arguments. They should be viewed as the first stage of this program.

Proof of Proposition A The proof of Proposition A is obtained by combining the next two lemmas. First of all, W_I is the isotopy subgroup of $\mathbb{E}^I$, since W_I clearly fixes $\mathbb{E}^I$. Also, by definition, $\mathbb{E}^I$ contains the set

$$\mathcal{C}_I = \left\{ t \in \mathbb{E} \;\middle|\; \begin{array}{l} (t, \alpha_i) = 0 \text{ for } i \in I \\ (t, \alpha_i) > 0 \text{ for } i \notin I \end{array} \right\}$$

whose isotropy group was shown in §5-2 to be W_I. It follows from this characterization of W_I as the isotropy subgroup for $\mathbb{E}^I$ that:

Lemma A *$c_I \in W$ if and only if $c_I \in W_I$.*

Because c_I fixes $\mathbb{E}^I$, it is equivalent to assert that c_I belongs to W, and that c_I belongs to the isotropy subgroup (in W) of $\mathbb{E}^I$.

Secondly, we can show that the criterion for c_I to belong to W_I is the same as that given in Lemma 27-2, namely, letting Δ_I be the parabolic subroot system defined as above, then:

Lemma B *$c_I \in W_I$ if and only if Δ_I is a disjoint union (repetitions allowed) of A_1, B_k, D_{2k}, E_7, E_8, F_4, $G_2(2k)$, H_3, H_4.*

To see why this equivalence holds, observe that, since the action of W_I on $\mathbb{E}$ respects the decomposition $\mathbb{E} = \mathbb{E}^I \oplus \mathbb{E}_I$, and since W_I fixes $\mathbb{E}^I$ pointwise, we have an inclusion

$$W_I \subset O(\mathbb{E}_I) \subset O(\mathbb{E}).$$

We can also write

$$\Delta_I = \Delta \cap \mathbb{E}_I.$$

Then $\Delta_I \subset \mathbb{E}_I$ is a root system for $W_I \subset O(\mathbb{E}_I)$, i.e., $W_I = W(\Delta_I)$. And when we consider the action of c_I on $\mathbb{E}_I$, we have $c_I = -1$. So the question of when $c_I \in W_I$ is answered by the criterion given in Lemma 27-2.

Proof of Proposition B First of all, since $\mathbb{E}_I$ and $\mathbb{E}^I$ are orthogonal, they determine each other. Also, $\mathbb{E}^I$ and $\mathbb{E}_I$ clearly determine c_I, and vice versa. By slightly extending these assertions we have

Lemma C *Given $\varphi \in W$ and $I, J \subset \{1, \ldots, \ell\}$, then the following are equivalent:*

(i) $\varphi c_I \varphi^{-1} = c_J$;
(ii) $\varphi \cdot \mathbb{E}_I = \mathbb{E}_J$;
(iii) $\varphi \cdot \mathbb{E}^I = \mathbb{E}^J$.

We now turn to the proof of Proposition B. By Proposition 5-3, we know that (ii), (iii) and (iv) of Proposition B are equivalent. So we only have to show (i) of Proposition B is equivalent to any of these. We shall prove the equivalence of (i) and (iii) by using Lemma C.

First of all, assume that c_I and c_J are conjugate. If $\varphi c_I \varphi^{-1} = c_J$, then, by Lemma C, $\varphi \cdot \mathbb{E}_I = \mathbb{E}_J$. The identities $\Delta_I = \Delta \cap \mathbb{E}_I$ and $\Delta_J = \Delta \cap \mathbb{E}_J$ then force $\varphi \cdot \Delta_I = \Delta_J$.

Conversely, assume that $\varphi \cdot \Delta_I = \Delta_J$. Since Δ_I and Δ_J span $\mathbb{E}_I$ and $\mathbb{E}_J$, respectively, it follows that $\varphi \cdot \mathbb{E}_I = \mathbb{E}_J$. By Lemma C, $\varphi c_I \varphi^{-1} = c_J$.

27-4 Conjugacy classes of involutions

In this section, we show that every involution in a reflection group is always conjugate to an involution of the type c_I defined in §27-3. So we can understand arbitrary involutions via the involutions $\{c_I\}$. In Chapter 28, we shall use this approach to produce an effective algorithm for classifying conjugacy classes of involutions. This agenda will be explained in more detail in §27-5.

Given an involution $\tau\colon \mathbb{E} \to \mathbb{E}$ where $(\tau \cdot x, \tau \cdot y) = (x, y)$ for all $x, y \in \mathbb{E}$, we have an orthogonal decomposition $\mathbb{E} = \mathbb{E}^\tau \oplus \mathbb{E}_\tau$ of eigenspaces, where

$$\mathbb{E}^\tau = \{x \in \mathbb{E} \mid \tau \cdot x = x\}$$
$$\mathbb{E}_\tau = \{x \in \mathbb{E} \mid \tau \cdot x = -x\}.$$

Examples:

(a) Given a reflection $\tau = s_\alpha$, then $\mathbb{E}_\tau = \mathbb{R}\alpha$ and $\mathbb{E}^\tau = H_\alpha$;
(b) Given the involution $\tau = c_I$ defined in §27-3, then $\mathbb{E}_\tau = \mathbb{E}_I$ and $\mathbb{E}^\tau = \mathbb{E}^I$.

The subspaces $\mathbb{E}^\tau$ and $\mathbb{E}_\tau$ are always orthogonal. Suppose that $\tau \cdot x = x$ and $\tau \cdot y = -y$. Then $(x, y) = (\tau \cdot x, \tau \cdot y) = (x, -y) = -(x, y)$. Thus $(x, y) = 0$. So the involution is completely determined by specifying the subspace $\mathbb{E}_\tau \subset \mathbb{E}$ or the subspace $\mathbb{E}^\tau \subset \mathbb{E}$. The following lemma (which is analogous to Lemma 27-3C) summarizes the above discussion.

Lemma A *Given involutions $\tau, \tau' \in W$, then, for any $\varphi \in W$, the following are equivalent:*

(i) $\varphi \tau \varphi^{-1} = \tau'$;
(ii) $\varphi \cdot \mathbb{E}_\tau = \mathbb{E}_{\tau'}$;
(iii) $\varphi \cdot \mathbb{E}^\tau = \mathbb{E}^{\tau'}$.

We now show that, if we work up to conjugacy, then the choice of $\mathbb{E}^\tau$ (and hence of τ) can be reduced to canonical choices. Furthermore, as we shall see, restricting to these canonical choices is the key to classifying involutions. Choose a reflection group $W \subset O(\mathbb{E})$ with root system $\Delta \subset \mathbb{E}$. Choose a fundamental system $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$ of Δ. For each subset $I \subset \{1, \ldots, \ell\}$, let

$$\mathbb{E} = \mathbb{E}^I \oplus \mathbb{E}_I$$

be the orthogonal decomposition defined in §27-3 and let $c_I \colon \mathbb{E} \longrightarrow \mathbb{E}$ denote the involution defined by

$$c_I = \begin{cases} 1 \text{ on } \mathbb{E}^I \\ -1 \text{ on } \mathbb{E}_I. \end{cases}$$

The next proposition tells us that, up to conjugacy, every involution can be identified with c_I for some I.

Proposition *Given an involution $\tau \in W$, there exists $\varphi \in W$ and $I \subset \{1, \ldots, \ell\}$ such that $\varphi\tau\varphi^{-1} = c_I$.*

Proof In order to prove the proposition it suffices, by the above lemma, to show that there exists $\varphi \in W$ and $I \subset \{1, \ldots, \ell\}$, where

$$\varphi \cdot \mathbb{E}^\tau = \mathbb{E}^I.$$

As in §5-2, we consider the decomposition of $\mathbb{E}$ into cells, and the action of W on that decomposition. As explained in §5-2, a cell in $\mathbb{E}$ is determined by introducing, for each $\alpha \in \Delta$, one of the three constraints:

$$(\alpha, x) = 0 \quad \text{or} \quad (\alpha, x) > 0 \quad \text{or} \quad (\alpha, x) < 0.$$

The nontrivial sets obtained by such constraints provide a decomposition of $\mathbb{E}$ into disjoint cells.

It is also true that $\mathbb{E}^\tau$ is a union of cells. It will be shown in §30-2 that there are roots $\{\alpha_1, \ldots, \alpha_k\}$ such that

$$\mathbb{E}^\tau = \bigcap_{i=1}^{k} H_{\alpha_i} = \{x \in \mathbb{E} \mid (\alpha_i, x) = 0 \text{ for } i = 1, \ldots, k\}.$$

Consequently, $\mathbb{E}^\tau$ is the union of the cells whose constraints include

$$(\alpha_i, x) = 0 \quad \text{for } i = 1, \ldots, k.$$

In particular, $\mathbb{E}^\tau$ must contain a cell S containing a basis of $\mathbb{E}^\tau$. Otherwise, every cell in $\mathbb{E}^\tau$ must be contained in a hyperplane of $\mathbb{E}^\tau$. But since $\mathbb{E}^\tau$ is covered by cells, this would mean that $\mathbb{E}^\tau$ would be the union of a finite number of hyperplanes, impossible by Lemma 3-3A.

For each $I \subset \{1, \ldots, \ell\}$, we have the cell

$$C_I = \left\{ t \in \mathbb{E} \;\middle|\; \begin{array}{l} (t, \alpha_i) = 0 \text{ for } i \in I \\ (t, \alpha_i) > 0 \text{ for } i \notin I. \end{array} \right\}.$$

Every cell in $\mathbb{E}$ is of the form $\varphi \cdot C_I$ for a unique choice of $\varphi \in W$ and C_I. So we can pick $\varphi \in W$ such that

$$\varphi \cdot S = C_I$$

for some $I \subset \{1, \ldots, \ell\}$. Observe that we have the inclusion $C_I \subset \mathbb{E}^I$, and C_I spans $\mathbb{E}^I$. So we must have $\varphi \cdot \mathbb{E}^\tau = \mathbb{E}^I$. ∎

27-5 Conjugacy classes and Coxeter graphs

Let $W \subset O(\mathbb{E})$ be a reflection group with root system $\Delta \subset \mathbb{E}$. Let $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$ be a fundamental system of Δ. We have now reduced an arbitrary involution to the case of an involution of type c_I. The rest of this chapter, as well as all of Chapter 28, will be devoted to the study of the conjugacy classes of such elements. It was explained in §27-3 how there are two questions to consider for such a classification:

(Q-1) When does $c_I \in W$?
(Q-2) Given $c_I, c_J \in W$, when are they conjugate in W?

In this section, and in Chapter 28, we explain how both questions can be reduced to facts about the Coxeter graph of Δ. In §27-3, it was explained how questions (Q-1) and (Q-2) can be answered by determining the W-equivalence classes of subsets of Σ. In Chapter 28, we do two more things:

(i) An effective algorithm will be developed for classifying W-equivalence classes.
(ii) It will be shown how the Coxeter graph can be used as a very effective visual aid in implementing this algorithm.

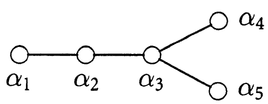
The point of using Coxeter graphs is that the elements of Σ can be identified with the vertices of the Coxeter graph. Thus the Coxeter graph provides a visual display of Σ and its subsets. This will make it easy both to pick out the subsets of Σ satisfying certain properties, and to determine when two of these subsets are equivalent. So the Coxeter graph is a heuristic device for carrying out certain arguments. The main content of the rest of this section illustrates how Coxeter graphs can be used to answer (Q-1) and (Q-2).

Question (Q-1) Given $I \subset \{1, \ldots, \ell\}$, we have the parabolic root system $\Delta_I \subset \Delta$ with fundamental system $\Sigma_I = \{\alpha_i \mid i \in I\}$. Proposition 27-3A indicates the type of restrictions that have to be imposed on Σ_I and Δ_I in order to have $c_I \in W$. If Δ_I is irreducible, then we must have

$$(*) \qquad \Delta_I = A_1, B_k, D_{2k}, E_7, E_8, F_4, G_2(2k), H_3, H_4.$$

So, given $\Sigma \subset \Delta$, we want the subsets $\Sigma_I \subset \Sigma$, where Δ_I is a disjoint union of these root systems. This is easily determined by looking at the Coxeter graph of Δ. If we identify Σ with the vertices of the graph, then the Coxeter graph of any Δ_I is the subgraph with the set Σ_I as vertices. We proceed by deleting nodes and determining which deletions give rise to (a union of) graphs from the above list.

Example 1: Consider the reflection group $W(D_5)$. Its Coxeter graph is



The following subgraphs of D_5 are the ones whose type appear in $(*)$ above.

$$A_1 = \{\alpha_1\}, \{\alpha_2\}, \{\alpha_3\}, \{\alpha_4\}, \{\alpha_5\}$$

$$A_1 \coprod A_1 = \{\alpha_1, \alpha_3\}, \{\alpha_1, \alpha_4\}, \{\alpha_1, \alpha_5\}, \{\alpha_2, \alpha_4\}, \{\alpha_2, \alpha_5\}, \{\alpha_4, \alpha_5\}$$

$$A_1 \coprod A_1 \coprod A_1 = \{\alpha_1, \alpha_4, \alpha_5\}, \{\alpha_2, \alpha_4, \alpha_5\}$$

$$D_4 = \{\alpha_2, \alpha_3, \alpha_4, \alpha_5\}.$$

Thus each involution in $W(D_5)$ is represented by the involution c_I, where I is the indexing set for one of the above subsets of $\Sigma = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5\}$. We are still left with the problem of determining when two of the above subsets determine c_I which are conjugate. That is the question posed by (Q-2).

Question (Q-2) This second question can also be reduced to manipulations involving Coxeter graphs, but it will take all of Chapter 28 to justify that fact. It was shown in Proposition 27-3B that the conjugacy of c_I and c_J in W is equivalent to the W-equivalence of Σ_I and Σ_J. In Chapter 28, we explain how the property of Σ_I and Σ_J being W-equivalent can be converted into the more explicit (although technical) property of their being related by a series of "elementary equivalences". This technical condition is easier to employ for explicit calculations. Notably, elementary equivalences can be analyzed by using Coxeter graphs. Thus by the end of Chapter 28 (Q-2) will be reduced to manipulations involving Coxeter graphs.

Example 2: If we again consider the reflection group $W(D_5)$, then, once we have established our machinery of elementary equivalences, we shall be able to easily show that many of the subsets $\Sigma_I \subset \Sigma$ described above determine conjugate c_I. Once we eliminate such redundancies, we are left with the following list:

$$A_1 = \{\alpha_1\}$$

$$A_1 \coprod A_1 = \{\alpha_1, \alpha_3\}, \{\alpha_4, \alpha_5\}$$

$$A_1 \coprod A_1 \coprod A_1 = \{\alpha_1, \alpha_4, \alpha_5\}$$

$$D_4 = \{\alpha_2, \alpha_3, \alpha_4, \alpha_5\}.$$

So there are five conjugacy classes of involutions in $W(D_5) = (\mathbb{Z}/2\mathbb{Z})^4 \rtimes \Sigma_5$. Of course, we still have to justify the above remarks. We shall return to this example in §28-5.

28 Elementary equivalences

Let W be a reflection group. The concept of W equivalences was introduced in §5-3. It was then shown in §27-4 that determining the conjugacy classes of involutions in W reduces to determining the W-equivalence classes of the subsets of any fundamental system of the root system of W. This chapter is devoted to the study of such equivalence classes. The results are based on the work of Deodhar [1], Richardson [1] and Springer [4]. We shall introduce the concept of elementary equivalences and show that every W equivalence can be decomposed as a series of elementary equivalences. Elementary equivalences have the advantage of being easily visualized. They can be described through symmetries of certain Coxeter graphs. As a consequence, W equivalences become easier to understand.

28-1 Summary

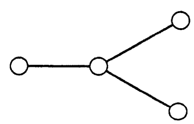
Let $W \subset O(\mathbb{E})$ be a Euclidean reflection group with root system $\Delta \subset \mathbb{E}$. Let $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$ be a fundamental system of Δ. The concept of W equivalence was introduced in §5-3. In this chapter, we study W equivalences between subsets of Σ. We shall reduce such equivalences to a condition that is more technical, but easier to employ for explicit calculations.

Our motivation for this study comes from the discussion in Chapter 27. For each set $I \subset \{1, \ldots, \ell\}$, we have the involution

$$c_I \colon \mathbb{E} \to \mathbb{E},$$

as well as the parabolic subgroup $W_I = W(\Delta_I)$ with root system Δ_I and fundamental system Σ_I. We showed in §27-4 that every involution in W is conjugate (in W) to some c_I. So classifying conjugacy classes of involutions in W amounts to classifying the conjugacy classes of the c_I belonging to W. It was also explained how the question of c_I and c_J being conjugate in W reduces to the question of Σ_I and Σ_J being W-equivalent. We shall apply our study of W equivalences to this question.

The goal is to understand W equivalences in terms of symmetries of Coxeter graphs. If we want to visualize W equivalences in some elementary way, then looking at symmetries of Coxeter graphs is an obvious strategy. The attraction of such symmetries is that they are easy to understand and easy to determine. For example, the symmetries of the graph D_4



clearly form the symmetric group Σ_3.

We begin by observing that symmetries of the Coxeter graph of Σ can be used to define equivalences between subsets of Σ. If we identify Σ with the vertices of the Coxeter graph, then the subsets Σ_I and Σ_J of Σ can be regarded as being

equivalent whenever there exists a symmetry σ of the graph such that $\sigma \cdot \Sigma_I = \Sigma_J$. Because it is easy to determine Coxeter graph symmetries, it is also easy to decide what subsets of Σ are equivalent in this fashion.

We shall use such equivalences to understand W equivalences. Actually, we must deal with a modification, or extension, of the above type of equivalence if we want to obtain W equivalences. Specifically, we must consider equivalences in Σ induced by symmetries of subgraphs of the Coxeter graph. In other words, we shall deal with "local" equivalences, rather than with the "global" equivalences described above. The point is that we are forced to consider such symmetries if we want to obtain W equivalences because an equivalence induced by a symmetry of the entire Coxeter graph of Σ could never be a W equivalence. A nontrivial permutation of Σ is never realized by an element of W. (If $\varphi \in W$ maps Σ to itself, then, by Theorem A of §4-3, $\ell(\varphi) = 0$ and, so, $\varphi = 1$.) On the other hand, "local" symmetries, i.e., of subgraphs, can in some cases be realized by elements of W.

We shall focus on a particular family of such local equivalences called "elementary equivalences". These equivalences will suffice for our purposes. It will be shown that they are W equivalences, and that any W equivalence can be decomposed into a series of elementary equivalences. So we shall have achieved our goal of visualizing W equivalences in terms of Coxeter graphs.

The discussion in the rest of this chapter will consist of defining elementary equivalences and illustrating how useful they are in understanding W equivalences. Notably, arbitrary W equivalences can be decomposed as a composite of elementary equivalences. Moreover, elementary equivalences are amenable to analysis via the Coxeter diagram of W.

28-2 Equivalences via Coxeter graph symmetries

In all that follows, let $W = W(\Delta)$ be a finite reflection group with root system Δ. Let $\Sigma \subset \Delta$ be a fixed fundamental system for Δ. As in §27-1, let ω_Σ be the element of greatest length in W (with respect to Σ) and write

$$\omega_\Sigma = -\tau_\Sigma,$$

where τ_Σ is an involution of Σ (and of the Coxeter graph of Σ). In the irreducible case, τ_Σ is a nontrivial involution when $\Delta = A_k$ $(k \geq 2)$, D_{2k+1}, E_6 or $G_2(2k+1)$.

By passing to the parabolic subgroups of W, we can generalize τ_Σ and obtain a whole family of Coxeter graph involutions related to elements of W. Given $K \subset \{1, \ldots, \ell\}$, let

$$\omega_K \in W_K$$

be the element of greatest length with respect to the fundamental system Σ_K of Δ_K. We can consider $\omega_K \in W$. As above, write

$$\omega_K = -\tau_K,$$

where τ_K is an involution. Then τ_K maps Σ_K to itself. As above, we have the property that, for Σ_K irreducible, the action of τ_K on Σ_K is nontrivial if and only

if $\Delta_K = A_k$ $(k \geq 2)$, D_{2k+1}, E_6 or $G_2(2k+1)$. Our interest in the involutions $\{\tau_K\}$ lies in the fact that subsets of Σ_K equivalent under τ_K are also W-equivalent. This follows from:

Lemma *Given $\Sigma_I, \Sigma_J \subset \Sigma_K$ if $\tau_K \cdot \Sigma_I = \Sigma_J$, then $(\omega_K\omega_I) \cdot \Sigma_I = \Sigma_J$.*

Proof Suppose $\tau_K \cdot \Sigma_I = \Sigma_J$. By definition $\omega_I \cdot \Sigma_I = -\Sigma_I$. So

$$(\omega_K\omega_I) \cdot \Sigma_I = -\tau_K \cdot (-\Sigma_I) = \tau_K \cdot \Sigma_I = \Sigma_J.$$ ■

We now have a potentially large number of W equivalences induced by Coxeter graph symmetries.

Remark $\omega_K\omega_I$ is not a permutation of Σ. It only maps the subset Σ_I to the subset Σ_J. Also, unlike τ_K, $\omega_K\omega_I$ need not be an involution.

28-3 Elementary equivalences

We are actually only interested in a special case of the above equivalences. This is the case $\Sigma_I \subset \Sigma_K$, where

$$\Sigma_K = \Sigma_I \coprod \{\alpha\}$$

for some $\alpha \in \Sigma - \Sigma_I$. The element

$$\sigma(I, \alpha) = \omega_K\omega_I$$

maps Σ_I to a subset Σ_J of Σ_K. We call $\sigma(I, \alpha)$ an *elementary W equivalence* and also say that Σ_I and Σ_J are related by an elementary equivalence. We adopt the notation

$$\Sigma_I \mapsto \Sigma_J$$

to indicate this elementary equivalence.

We can slightly rephrase the above definition. Σ_I and Σ_J are related by an elementary equivalence if $\Sigma_I, \Sigma_J \subset \Sigma_K$, where Σ_K can be decomposed

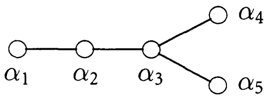
$$\Sigma_K = \Sigma_I \coprod \{\alpha\} = \Sigma_J \coprod \{\beta\}$$

and τ_K satisfies

$$\tau_K \cdot \Sigma_I = \Sigma_J.$$

It is straightforward to determine, for a given subset $\Sigma_I \subset \Sigma$, exactly what other subsets of Σ are related to it through an elementary equivalence. We take each $\alpha \in \Sigma - \Sigma_I$, let $\Sigma_K = \Sigma_I \coprod \{\alpha\}$ and then determine the effect of τ_K on Σ_I. By our previous comments, we need only concern ourselves with the cases where Σ_K is of the type A_k $(k \geq 2)$, D_{2k+1}, E_6 or $G_2(2k+1)$.

Example: Consider the case $\Delta = D_5$ with Coxeter graph



The following equivalences are concerned with three different types of root systems. In (i) we deal with equivalences between root systems of type A_1. In (ii) we deal with root systems of type A_2. In (iii) and (iv) we consider root systems of type $A_1 \coprod A_1$.

(i) For $\Sigma_I = \{\alpha_3\}$, we have the elementary equivalences

$$\{\alpha_3\} \mapsto \{\alpha_2\} \quad \text{and} \quad \{\alpha_3\} \mapsto \{\alpha_4\} \quad \text{and} \quad \{\alpha_3\} \mapsto \{\alpha_5\}.$$

(ii) For $\Sigma_I = \{\alpha_1, \alpha_2\}$, we have the elementary equivalence

$$\{\alpha_1, \alpha_2\} \mapsto \{\alpha_2, \alpha_3\}.$$

(iii) For $\Sigma_I = \{\alpha_1, \alpha_3\}$, we have the elementary equivalences

$$\{\alpha_1, \alpha_3\} \mapsto \{\alpha_1, \alpha_4\} \quad \text{and} \quad \{\alpha_1, \alpha_3\} \mapsto \{\alpha_1, \alpha_5\}.$$

(iv) For $\Sigma_I = \{\alpha_4, \alpha_5\}$, there are no elementary equivalences between it and any other subset of Σ.

The above discussion can easily be extended to show that all subroot systems of type A_1, or of type A_2, are linked by elementary equivalences. On the other hand, the root systems of type $A_1 \coprod A_1$ fall into two classes with (iii) and (iv) providing representatives.

By further extending these arguments, we can show that, except for subroot systems of type $A_1 \coprod A_1$, any two subsets from Σ of the same type are linked by a series of elementary equivalences. It is instructive to convince ourselves that all subroot systems of type $A_1 \coprod A_2$ are linked by elementary equivalences.

28-4 Decomposition of W equivalences into elementary equivalences

This section will be devoted to proving the following:

Proposition *If Σ_I and Σ_J are W-equivalent, then they are related by a series of elementary equivalences*

$$\Sigma_I = \Sigma_{I_1} \mapsto \Sigma_{I_2} \mapsto \cdots \mapsto \Sigma_{I_{k-1}} \mapsto \Sigma_{I_k} = \Sigma_J.$$

Suppose that $\varphi \cdot \Sigma_I = \Sigma_J$. We begin by reducing the construction of the desired series of elementary equivalences to a statement about the action of W on the root system Δ.

Part I First of all, to construct the series of elementary equivalences, it suffices, by an inductive argument on length in W (defined with respect to Σ), to show that we can pick $\alpha \in \Sigma - \Sigma_I$ so that $\sigma = \sigma(I, \alpha)$ satisfies

$$(*) \qquad \ell(\varphi\sigma^{-1}) < \ell(\varphi).$$

Let $\widehat{\varphi} = \varphi\sigma^{-1}$ and $\Sigma_{I'} = \sigma \cdot \Sigma$. By definition, we have

$$\Sigma_I \mapsto \Sigma_{I'}.$$

By applying the induction hypothesis to $\widehat{\varphi} \cdot \Sigma_{I'} = \Sigma_J$, we can also produce a series of elementary equivalences

$$\Sigma_{I'} \mapsto \Sigma_L \mapsto \cdots \mapsto \Sigma_M \mapsto \Sigma_J.$$

The proposition then follows from combining these two series of elementary equivalences.

Part II Next, let Δ^+ be the positive roots with respect to Σ and consider the set

$$\Delta(\varphi) = \{\alpha \in \Delta^+ \mid \varphi \cdot \alpha < 0\}$$

defined in §4-3. The second stage in the proof of the proposition is to demonstrate that we can reduce $(*)$ to a statement about the set $\Delta(\varphi)$. Recall that the length of φ (with respect to Σ) is given by

$$\ell(\varphi) = |\Delta(\varphi)|.$$

To prove $(*)$, it suffices to prove that we can choose $\alpha \in \Sigma - \Sigma_I$ such that $\sigma = \sigma(I, \alpha)$ satisfies

$$(**) \qquad \Delta(\sigma) \subset \Delta(\varphi)$$

because the inequality $|\Delta(\varphi\sigma^{-1})| < |\Delta(\varphi)|$ is equivalent to $(*)$. And $(**)$ suffices to force this inequality. To see this, pick $x \in \Delta(\varphi\sigma^{-1})$, i.e., $x \in \Delta^+$ and $\varphi\sigma^{-1} \cdot x < 0$. First of all, we have

(a) $\sigma^{-1} \cdot x > 0$.

The only other possibility is that $\sigma^{-1} \cdot x < 0$. However, this would mean that $x \in \Delta(\sigma^{-1})$. And, since σ^{-1} maps $\Delta(\sigma^{-1})$ to $-\Delta(\sigma)$ (use $\sigma \cdot \sigma^{-1} = 1$), and since φ maps $-\Delta(\sigma)$ into Δ^+ (use $(**)$), we would then have $\varphi\sigma^{-1} \cdot x > 0$, a contradiction.

Since $\varphi\sigma^{-1} \cdot x < 0$, we have

(b) $\sigma^{-1} \cdot x \in \Delta(\varphi)$.

On the other hand, we also have

(c) $\sigma^{-1} \cdot x \notin \Delta(\sigma)$.

For if $\sigma^{-1} \cdot x \in \Delta(\sigma)$, then $x = \sigma(\sigma^{-1} \cdot x) < 0$, a contradiction.

It follows from (b) and (c) that $|\Delta(\varphi\sigma^{-1})| \leq |\Delta(\varphi)| - |\Delta(\sigma)|$.

Part III We begin by choosing α. Since $\ell(\varphi) > 0$, there exists $\alpha \in \Sigma$ such that $\varphi \cdot \alpha < 0$. Since $\varphi \cdot \Sigma_I \subset \Sigma$, we must have $\alpha \in \Sigma - \Sigma_I$. Let $\sigma = \sigma(I, \alpha)$ where α is chosen as above. In all that follows let

$$\Sigma_K = \Sigma_I \coprod \{\alpha\}.$$

Inclusion $(**)$ follows by combining the next two lemmas.

Lemma A $\Delta(\sigma) = \Delta_K^+ - \Delta_I^+$.

Proof It follows from properties (H-1) and (H-2) of §27-1 that ω_I interchanges Δ_I^+ and Δ_I^- and permutes $\Delta^+ - \Delta_I^+$, whereas ω_K interchanges Δ_K^+ and Δ_K^- and permutes $\Delta^+ - \Delta_K^+$. The element $\sigma = \omega_K \omega_I$ then clearly satisfies the lemma. ∎

Lemma B $\Delta_K^+ - \Delta_I^+ \subset \Delta(\varphi)$.

Proof Pick $\beta \in \Delta_K^+ - \Delta_I^+$. We want to show that $\varphi \cdot \beta < 0$. We can write

$$\beta = c\alpha + \gamma,$$

where $c > 0$ and $\gamma \in \Delta_I^+$. So

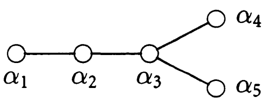
$$\varphi \cdot \beta = c(\varphi \cdot \alpha) + \varphi \cdot \gamma.$$

Since $\varphi \cdot \Sigma = \Sigma$, it is also true that $\varphi \cdot \Delta_I^+ = \Delta_J^+$ and $\varphi \cdot \Delta_I = \Delta_J$. So the relations $\gamma \in \Delta_J^+$ and $\alpha \notin \Delta_I$ translate into

$$\varphi \cdot \gamma \in \Delta_J^+ \quad \text{and} \quad \varphi \cdot \alpha \notin \Delta_J.$$

Now $\varphi \cdot \alpha < 0$, with $\varphi \cdot \alpha \notin \Delta_J$, forces one of the fundamental roots from $\Sigma - \Sigma_J$ to appear in the expansion of $\varphi \cdot \alpha$ with a negative coefficient. Since $\varphi \cdot \gamma \in \Delta_J^+$, this fundamental root has the same property for $\varphi \cdot \beta$. We conclude that $\varphi \cdot \beta < 0$. ∎

Example: At the end of §28-3, we observed the existence of a number of elementary equivalences in the case of the root system $\Delta = D_5$ with Coxeter graph



We considered three different types of subroot systems: A_1, A_2, and $A_1 \coprod A_1$ in detail, and stated that we could extend the arguments to show that any two subsets from Σ of type A_1 or A_2 are linked by a series of elementary equivalences. On the other hand, the subroot systems of type $A_1 \coprod A_1$ divide into two groups represented by the sets $\{\alpha_1, \alpha_3\}$ and $\{\alpha_4, \alpha_5\}$. Because of the above proposition, we now know that these same results apply to W-equivalence classes of subsets of Σ of type A_1, A_2, and $A_1 \coprod A_1$.

28-5 Involutions

We now return to the topic that motivated the discussion of W equivalences and of elementary equivalences, namely the classification of involutions in a reflection group up to conjugacy. It follows from Questions (Q-1) and (Q-2) listed in §27-3, and all the subsequent discussion of these questions in Chapters 27 and 28, that we now have an effective algorithm for classifying conjugacy classes of involutions in a reflection group. In §27-5, we explained how these questions could be handled

in terms of Coxeter graphs. In Chapter 28, we have developed the machinery needed to make the arguments. Let W be a reflection group with root system Δ and fundamental system Σ.

(i) We can draft a complete list (with possible redundancies) of conjugacy classes of involutions in W by finding all subsets $\Sigma_I \subset \Sigma$ that possess a Coxeter graph that is a disjoint union of graphs of the following types:

$$A_1,\ B_k,\ D_{2k},\ E_7,\ E_8,\ F_4,\ G_2(2k),\ H_3,\ H_4.$$

This follows from the discussion in §27-5. For each such I, the involution c_I lies in W. And these involutions represent all the conjugacy classes of involutions in W.

(ii) We can eliminate redundancies in the above list of conjugacy classes by determining which subsets $\Sigma_I \subset \Sigma$ are linked to each other by elementary equivalences. If two subsets of Σ are so linked, then the corresponding involutions c_I are conjugate and, thus, represent the same conjugacy classes.

There is an explicit algorithm for determining the elementary equivalences. We determine all the ways the sets $\Sigma_I \subset \Sigma$ from the list in (i) can be extended, by adding one more root $\alpha \in \Sigma$ to form a subset $\Sigma_K = \Sigma_I \cup \{\alpha\}$ of type

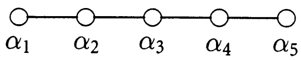
$$A_k\ (k \geq 2),\ D_{2k+1},\ E_6,\ G_2(2k+1).$$

Each such extended set has a nontrivial involution that carries Σ_I to another subset of Σ_K (and hence of Σ) of the same type. These transformations of subsets of Σ are the elementary equivalences. All this follows from Proposition 27-4 and the discussion in §28-2.

(iii) Finally, Coxeter graphs provide a visual aid for all the above. We have already provided examples of how to carry out the above program using Coxeter graphs.

Example 1: The Group $W(A_5) = \Sigma_6$ Since every element of a symmetric group can be written as a product of disjoint cycles, and since two elements of the same "cycle type" are conjugate, it is easy to determine the involutions in $W(A_5)$. There are three conjugacy classes represented by the elements $(1,2)$, $(1,2)(3,4)$ and $(1,2)(3,4)(5,6)$, respectively. Let us now see how this same result can be deduced using our current machinery.

The group $W(A_5)$ has Coxeter graph



where $\Sigma = \{\alpha_1, \ldots, \alpha_5\}$ is the fundamental graph of a root system of $W(A_5)$. The subsets of Σ satisfying the restrictions on type, as given in (i) above, are:

$$A_1 = \{\alpha_1\}, \{\alpha_2\}, \{\alpha_3\}, \{\alpha_4\}, \{\alpha_5\}$$

$$A_1 \coprod A_1 = \{\alpha_1, \alpha_3\}, \{\alpha_1, \alpha_4\}, \{\alpha_1, \alpha_5\}, \{\alpha_2, \alpha_4\}, \{\alpha_2, \alpha_5\}, \{\alpha_3, \alpha_5\}$$

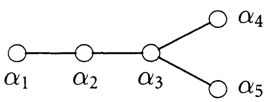
$$A_1 \coprod A_1 \coprod A_1 = \{\alpha_1, \alpha_3, \alpha_5\}.$$

It is easy to construct elementary equivalences linking any two of the above subsets of the same type. For example, in the $A_1 \coprod A_1$ case, we have the elementary equivalences

$$\{\alpha_1, \alpha_3\} \mapsto \{\alpha_1, \alpha_4\} \mapsto \{\alpha_1, \alpha_5\} \mapsto \{\alpha_2, \alpha_5\} \mapsto \{\alpha_3, \alpha_5\}.$$

It follows that the above subsets of Σ fall into three W-equivalence classes of type $A_1, A_1 \coprod A_1$ and $A_1 \coprod A_1 \coprod A_1$ respectively. So $W(A_5)$ has three conjugacy classes of involutions as stated.

Example 2: The Group $W(D_5) = (\mathbb{Z}/2\mathbb{Z})^4 \rtimes \Sigma_5$ This example was already discussed in §27-5. The pattern of involutions was sketched there, but not fully justified. This group has Coxeter graph



where $\Sigma = \{\alpha_1, \ldots, \alpha_5\}$ is a fundamental system for a root system of $W(D_5)$. It was shown in §27-5 that the following subsets of Σ satisfy the restrictions listed in (i) above:

$$A_1 = \{\alpha_1\}, \{\alpha_2\}, \{\alpha_3\}, \{\alpha_4\}, \{\alpha_5\}$$

$$A_1 \coprod A_1 = \{\alpha_1, \alpha_3\}, \{\alpha_1, \alpha_4\}, \{\alpha_1, \alpha_5\}, \{\alpha_2, \alpha_4\}, \{\alpha_2, \alpha_5\}, \{\alpha_4, \alpha_5\}$$

$$A_1 \coprod A_1 \coprod A_1 = \{\alpha_1, \alpha_4, \alpha_5\}, \{\alpha_2, \alpha_4, \alpha_5\}$$

$$D_4 = \{\alpha_2, \alpha_3, \alpha_4, \alpha_5\}.$$

At the end of §28-3 and §28-4, we discussed the elementary equivalences between certain subsets of Σ. By slightly extending these arguments, and using the relation between elementary equivalences and W equivalences, we can show that the above sets divide into five W-equivalence classes represented by:

$$A_1 = \{\alpha_1\}$$

$$A_1 \coprod A_1 = \{\alpha_1, \alpha_3\}, \{\alpha_4, \alpha_5\}$$

$$A_1 \coprod A_1 \coprod A_1 = \{\alpha_1, \alpha_4, \alpha_5\}$$

$$D_4 = \{\alpha_2, \alpha_3, \alpha_4, \alpha_5\}.$$

So there are five conjugacy classes of involutions in $W(D_5)$.

It is instructive to take the identity $W(D_5) = (\mathbb{Z}/2\mathbb{Z})^4 \rtimes \Sigma_5$ and use it to identify these five classes of involutions. The elements of $(\mathbb{Z}/2\mathbb{Z})^4 \rtimes \Sigma_5$ are determined up to conjugacy by their signed cycle type (see, for example, Carter [2]). The elements of $(\mathbb{Z}/2\mathbb{Z})^4 \rtimes \Sigma_5$ permute $\{\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4, \epsilon_5\}$ and also change their signs. A signed cycle keeps track of these two operations. For example, if φ permutes $\{\epsilon_1, \epsilon_4, \epsilon_5, \epsilon_3\}$ (in that order) and $\varphi^4 = 1$, then φ is the positive cycle $(1,4,5,3)$, whereas if $\varphi^4 = -1$, then φ is the negative cycle $-(1,4,5,3)$. The conjugacy classes of $(\mathbb{Z}/2\mathbb{Z})^4 \rtimes \Sigma_5$ are obtained by taking the cycle types involving an even number of negative cycles. There are five possibilities for involutions represented by the cycle types:

$$
\begin{array}{ll}
\{(1,2)\} & \{-(1),-(2)\} \\
\{(1,2),(3,4)\} & \{-(1,2),-(3,4)\} \\
\{-(1),-(2),-(3),-(4)\}. &
\end{array}
$$

29 Coxeter elements

Coxeter elements form a distinguished conjugacy class in each finite Euclidean reflection group. This chapter concerns their order. We shall show that, for an irreducible reflection group, the order of a Coxeter element can be expressed in terms of the associated root system. Coxeter elements will be treated again in Chapters 32 and 34 when we discuss regular elements. In this chapter, as a preliminary result, we shall prove that Coxeter elements are regular. The results of this chapter are independent of those in Chapters 27 and 28.

29-1 Coxeter elements

To define a Coxeter element, let $W \subset O(\mathbb{E})$ be the finite Euclidean reflection group associated to the root system $\Delta \subset \mathbb{E}$ and let $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$ be a fundamental system of Δ. Then

$$\omega = s_{\alpha_1} \cdots s_{\alpha_\ell}$$

is called a *Coxeter element*. There are many different Coxeter elements in W, since we can rearrange the elements in a fundamental system, as well as replace the given fundamental system by another.

Example: Let $V \subset \mathbb{R}^{\ell+1}$ be the subspace

$$V = \{(x_1, \ldots, x_{\ell+1}) \mid x_1 + \cdots + x_{\ell+1} = 0\}$$

and let $\Sigma_{\ell+1}$ act on V by permuting the coordinates. This action realizes $\Sigma_{\ell+1}$ as the finite reflection group $W(A_\ell)$. The Coxeter elements in $W(A_\ell) = \Sigma_{\ell+1}$ are the $\ell + 1$ cycles because the reflections in $\Sigma_{\ell+1}$ are the involutions (i, j). And, for any permutation $\{i_1, i_2, \ldots, i_{\ell+1}\}$ of $\{1, 2, \ldots, \ell + 1\}$, the involutions

$$\{(i_1, i_2), (i_2, i_3), \ldots, (i_\ell, i_{\ell+1})\}$$

are a set of fundamental reflections. So the element

$$(i_1, i_2)(i_2, i_3) \cdots (i_\ell, i_{\ell+1}) = (i_1, i_2, \ldots, i_{\ell+1})$$

is a Coxeter element.

It is well known that all of these Coxeter elements in $\Sigma_{\ell+1}$ are conjugate. In §29-2, we shall extend this result to Coxeter elements of any finite reflection group. We shall prove:

Theorem A *All the Coxeter elements of a finite Euclidean reflection group lie in the same conjugacy class.*

After proving the above result, most of the rest of Chapter 29 will be devoted to determining the order of Coxeter elements. The order of a Coxeter element

in an irreducible finite reflection group has a simple relation to the root system underlying the reflection group. Let

$$2N = \text{the number of elements in } \Delta.$$

Equivalently, N is the number of reflections in W. Sections §29-3 and §29-4 will be devoted to proving:

Theorem B *If a finite reflection group is irreducible, then the order of any Coxeter element is* $2N/\ell$.

The order of its Coxeter elements is called the *Coxeter number* of the group. By the theorem, the Coxeter number for each irreducible finite reflection group can be calculated from the root system underlying the reflection group. If we take the root systems given in §8-7 and calculate the Coxeter number $h = 2N/\ell$, then we obtain

A_ℓ	B_ℓ	D_ℓ	E_6	E_7	E_8	F_4	$G_2(m)$	H_3	H_4
$\ell+1$	2ℓ	$2\ell-2$	12	18	30	12	m	10	30

.

The Coxeter number is a fascinating one, arising in many contexts. It has already arisen twice in this book.

(1) In Chapter 12 we gave, for each irreducible crystallographic root system Δ, the expansion $\alpha_o = \sum_{i=1}^{\ell} h_i\alpha_i$, where $\{\alpha_1, \ldots, \alpha_\ell\}$ is a fundamental system of Δ and α_o is the "highest root" of Δ with respect to $\{\alpha_1, \ldots, \alpha_\ell\}$. In each case, the order of the Coxeter element in $W(\Delta)$ is $1 + \sum_{i=1}^{\ell} h_i$.

(2) In the table at the end of Chapter 14, we listed the degrees of the irreducible complex pseudo-reflection groups. The list includes all (real) reflection groups. For each of these real reflection group, the order of its Coxeter element is the highest degree. This relation will be verified in §32-2.

29-2 Coxeter elements are conjugate

In this section, we prove Theorem 29-1A. Let $W \subset O(\mathbb{E})$ be the finite Euclidean reflection group associated with the root system $\Delta \subset \mathbb{E}$. We want to show that any two Coxeter elements of W are conjugate. We begin by observing that, if we conjugate a Coxeter element, then we obtain another Coxeter element because, if $\varphi \in W$ and $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$ is a fundamental system, then $\varphi \cdot \Sigma = \{\varphi \cdot \alpha_1, \ldots, \varphi \cdot \alpha_\ell\}$ is another fundamental system. Moreover, by property (A-4) of §1-1,

$$\varphi s_{\alpha_1} \cdots s_{\alpha_\ell} \varphi^{-1} = s_{\varphi\cdot\alpha_1} \cdots s_{\varphi\cdot\alpha_\ell}.$$

This remark also shows that, in order to prove the theorem, it suffices to fix a fundamental system $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$ and show that all the Coxeter elements arising from different permutations of $\{\alpha_1, \ldots, \alpha_\ell\}$ are conjugate. For, by §4-6, any other fundamental system is of the form $\varphi \cdot \Sigma = \{\varphi \cdot \alpha_1, \ldots, \varphi \cdot \alpha_\ell\}$ for some

$\varphi \in W$. And, by the preceding paragraph, the Coxeter elements arising from $\varphi \cdot \Sigma$ are conjugate to those arising from Σ.

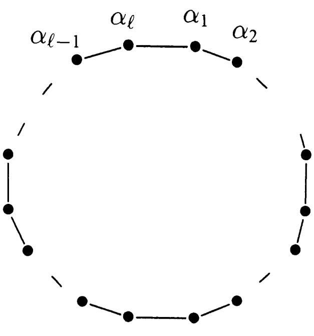
Consider a fixed fundamental system $\Sigma = \{\alpha_1, \dots, \alpha_\ell\}$ of Δ. The Coxeter graph of Δ was introduced in §8-7. Assume that the vertices in the Coxeter graph of Δ are labelled by $\{\alpha_1, \dots, \alpha_\ell\}$. We want to show:

Lemma *All the permutations of* $\{\alpha_1, \dots, \alpha_\ell\}$ *can be obtained by:*

(i) rotating, i.e., sending $\{\alpha_{i_1}, \dots, \alpha_{i_\ell}\}$ *to* $\{\alpha_{i_2}, \alpha_{i_3}, \dots, \alpha_{i_\ell}, \alpha_{i_1}\}$*;*
(ii) interchanging adjacent roots in $\{\alpha_{i_1}, \dots, \alpha_{i_\ell}\}$ *whose vertices in the Coxeter graph are not connected by an edge.*

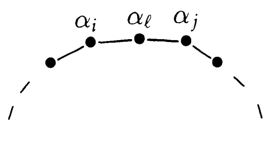
Both of the operations in the lemma give rise to conjugate Coxeter elements. In (i), $s_{\alpha_{i_1}} \cdots s_{\alpha_{i_\ell}}$ is conjugate to $s_{\alpha_{i_2}} \cdots s_{\alpha_{i_\ell}} s_{\alpha_{i_1}}$ via $s_{\alpha_{i_1}}$. In (ii), we have interchanged two adjacent reflections in $s_{\alpha_{i_1}} \cdots s_{\alpha_{i_\ell}}$ that commute with one another. So the Coxeter elements are not only conjugate, but also equal. Hence, if all permutations of $\{\alpha_1, \dots, \alpha_\ell\}$ can be obtained from operations (i) and (ii) of the lemma, then the Coxeter elements associated with the various permutations of $\{\alpha_1, \dots, \alpha_\ell\}$ will all be conjugate.

Proof of Lemma By (i), when we consider permutations of $\{\alpha_1, \dots, \alpha_\ell\}$, we can represent $\{\alpha_1, \dots, \alpha_\ell\}$ in circular fashion:

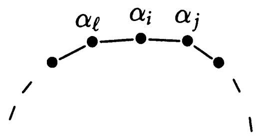


We are not concerned with the starting point, only the clockwise order of the roots on the circle. And we are reduced to showing that the roots can be arranged in any order on the circle by using (ii). We know that the Coxeter graph of a root system is a tree (see §8-2). So there exists a vertex in the Coxeter graph of Δ joined to at most one other vertex. Assume that α_ℓ is the label of this vertex.

If we delete α_ℓ, then, by induction, we can interchange the positions of $\{\alpha_1, \dots, \alpha_{\ell-1}\}$ on the circle in any fashion by using (ii). If we attempt to carry on these interchanges with α_ℓ present, then a potential obstruction arises when we want to interchange α_i and α_j (using (ii)) but α_ℓ separates them.



However, from the hypothesis required to use (ii), we know that the vertices of α_i and α_j (in the Coxeter graph of Δ) are not linked. Moreover, we also know that the vertex of α_ℓ is linked to at most one other vertex. So assume that it is not linked to the vertex of α_i. Then we can use (ii) to rearrange the vertices in the order



In particular, we have interchanged α_i and α_j. So the presence of α_ℓ is no impediment.

Finally, we can use (ii) to move α_ℓ to any desired position on the circle. For, by our choice of α_ℓ, there is at most one root that cannot be interchanged with α_ℓ by using (ii). So we simply have to choose the appropriate direction (clockwise or counterclockwise) in which to move α_ℓ around the circle so as to avoid the problem root.

29-3 A dihedral subgroup

This section and the next are devoted to determining the order of Coxeter elements. The goal is to verify Theorem 29-1B. Let us begin by observing that Theorem 29-1B holds in the case of planar reflection groups. These groups were studied in Chapter 1 and are dihedral groups. The planar reflection group D_m contains m reflections and m rotations. In particular, the Coxeter element is a rotation of order m. Theorem 29-1B asserts that the order of Coxeter element in D_m is $2N/\ell = 2m/2 = m$.

In the case of an arbitrary Euclidean reflection group $W(\Delta) \subset O(\mathbb{E})$, the order of Coxeter elements is determined by reducing to the case of the planar dihedral groups. In this section, we locate a plane $P \subset \mathbb{E}$ and a dihedral subgroup $D_m \subset W(\Delta)$ such that D_m maps P to itself, and the resulting action realizes D_m as a planar reflection group. In addition, the Coxeter element of D_m will also be a Coxeter element for $W(\Delta)$. The order of the Coxeter elements will then be determined in §29-4.

(I) The Elements τ_1 ***and*** τ_2 We can partition the fundamental system

$$\Sigma = \{\alpha_1, \ldots, \alpha_k\} \coprod \{\alpha_{k+1}, \ldots, \alpha_\ell\}$$

into two sets, with each set consisting of roots orthogonal to each other. To make such a choice, we use induction on the number of fundamental roots. To employ the induction hypothesis on Σ, remove a root α orthogonal to all but at most one root, partition the remaining roots in the required fashion, and then add α to the set to which it is orthogonal. How do we know such an α exists? We reuse some facts from §29-2. Identify the fundamental roots with the vertices of the Coxeter

graph of Δ. Since the Coxeter graph is a tree, it has a vertex α linked to at most one other vertex.

If we let

$$\tau_1 = s_{\alpha_1} \cdots s_{\alpha_k}$$

$$\tau_2 = s_{\alpha_{k+1}} \cdots s_{\alpha_\ell}.$$

Then $\omega = \tau_1\tau_2$ is a Coxeter element of W. Observe that the elements $\{s_{\alpha_1}, \ldots, s_{\alpha_k}\}$ commute with one another, as do the elements $\{s_{\alpha_{k+1}}, \ldots, s_{\alpha_\ell}\}$. So $(\tau_1)^2 = (\tau_1)^2 = 1$ and $\{\tau_1, \tau_2\}$ generate a dihedral subgroup

We want to construct a plane $P \subset \mathbb{R}^\ell$ on which τ_1 and τ_2 act as reflections. Let $V = \mathbb{R}^\ell$ and let

$$V = V^{\tau_1} \oplus V_{\tau_1}$$

$$V = V^{\tau_2} \oplus V_{\tau_2}$$

be the orthogonal decompositions of V into the $+1$ and -1 eigenspaces of τ_1 and τ_2, respectively. Finding a plane $P \subset \mathbb{R}^n$ on which τ_1 and τ_2 act as reflections is equivalent to finding a plane $P \subset \mathbb{R}^n$, where the intersection of P with each of V^{τ_1}, V^{τ_2}, V_{τ_1} and V_{τ_2} is nontrivial. Clearly, both τ_1 and τ_2 will map such a surface to itself and, in the process, act as reflections.

Let $\{\widehat{\alpha}_1, \ldots, \widehat{\alpha}_\ell\}$ be the dual basis of $\{\alpha_1, \ldots, \alpha_\ell\}$, i.e.,

$$(\alpha_i, \widehat{\alpha}_j) = \delta_{ij}.$$

Then:

Lemma A

(i) $\{\alpha_1, \ldots, \alpha_k\}$ *is a basis of* V_{τ_1} *and* $\{\alpha_{k+1}, \ldots, \alpha_\ell\}$ *is a basis of* V_{τ_2}*;*
(ii) $\{\widehat{\alpha}_1, \ldots, \widehat{\alpha}_k\}$ *is a basis of* V^{τ_2} *and* $\{\widehat{\alpha}_{k+1}, \ldots, \widehat{\alpha}_\ell\}$ *is a basis of* V^{τ_1}.

Proof Regarding (i), in view of the mutual orthogonality of the terms in $\{\alpha_1, \ldots, \alpha_k\}$, as well as those in $\{\alpha_{k+1}, \ldots, \alpha_\ell\}$, we have

$$s_{\alpha_i} \cdot \alpha_j = \begin{cases} \alpha_j \text{ for } j \neq i \\ -\alpha_j \text{ for } j = i \end{cases}$$

whenever both α_i and α_j lie in $\{\alpha_1, \ldots, \alpha_k\}$ or $\{\alpha_{k+1}, \ldots, \alpha_\ell\}$. Regarding (ii), that $(\alpha_i, \widehat{\alpha}_j) = 0$ for $i \neq j$ tells us

$$s_{\alpha_i} \cdot \widehat{\alpha}_j = \widehat{\alpha}_j \quad \text{for } i \neq j.$$

■

(II) The Matrices M ***and*** $I - M$ Next, consider the matrix

$$M = [(\alpha_i, \alpha_j)]_{\ell \times \ell}.$$

It can be viewed as the transition matrix whose columns express the basis $\{\alpha_i\}$ in terms of the dual basis $\{\widehat{\alpha}_i\}$. (For any $x \in V$, we have the identity $x = \sum_{i=1}^{\ell} (\alpha_i, x)\widehat{\alpha}_i$.) So if we work with respect to the basis $\{\widehat{\alpha}_i\}$, then it represents the linear map $M \colon V \to V$ defined by:

$$M \cdot \widehat{\alpha}_i = \alpha_i.$$

Thus M induces isomorphisms

$$(*) \qquad M \colon V^{\tau_1} \cong V_{\tau_2} \quad \text{and} \quad M \colon V^{\tau_2} \cong V_{\tau_1}.$$

Next, we consider the matrix $I - M$. By the orthogonality properties of the partition $\Sigma = \{\alpha_1, \ldots, \alpha_k\} \coprod \{\alpha_{k+1}, \ldots, \alpha_\ell\}$, the matrix M is of the form

$$M = \begin{bmatrix} I_k & A \\ A^t & I_{\ell-k} \end{bmatrix}.$$

Hence,

$$I - M = \begin{bmatrix} 0 & -A \\ -A^t & 0 \end{bmatrix}.$$

Since we are working with respect to the basis $\{\widehat{\alpha}_1, \ldots, \widehat{\alpha}_\ell\}$, it follows from Lemma A that

$$(**) \qquad I - M \text{ maps } V^{\tau_1} \text{ to } V^{\tau_2}, \text{ and vice versa.}$$

The matrices M and $I - M$ share the same eigenvectors, though not the same eigenvalues. The relation is

$$(I - M) \cdot x = \lambda x \quad \text{if and only if } M \cdot x = (-\lambda + 1)x.$$

As explained in Appendix C, there exists an orthogonal matrix T such that TMT^t is diagonal. In particular, M has eigenvectors. The matrix M also satisfies the hypothesis of Corollary A from Appendix C. Consequently, it satisfies the conclusion and we have:

Lemma B *M and $I - M$ have an eigenvector whose coefficients with respect to the basis $\{\widehat{\alpha}_1, \ldots, \widehat{\alpha}_\ell\}$ are positive.*

(III) The Plane P We shall construct the plane P by using the eigenvector of $I - M$ given in the preceding lemma. Suppose

$$(I - M) \cdot x = \lambda x,$$

where $\lambda \in \mathbb{R}$ and $x \in V$ and where the expansion $x = x_1\widehat{\alpha}_1 + \cdots + x_\ell\widehat{\alpha}_\ell$ satisfies

$$x_i > 0 \quad i = 1, \ldots, \ell.$$

It follows from Lemma A that there is a direct sum decomposition $V = V^{\tau_1} \oplus V^{\tau_2}$. Write

$$x = y + z,$$

where $y \in V^{\tau_1}$ and $z \in V^{\tau_2}$. Explicitly,

$$y = x_{k+1}\widehat{\alpha}_{k+1} + \cdots + x_\ell\widehat{\alpha}_\ell \quad \text{and} \quad z = x_1\widehat{\alpha}_1 + \cdots + x_k\widehat{\alpha}_k.$$

Let

$$P = \mathbb{R}y + \mathbb{R}z.$$

By construction (see Lemma A), P intersects V^{τ_1} and V^{τ_2}. So we are left with showing that P intersects both V_{τ_1} and V_{τ_2}. The identities $x = y + z$ and $(I - M) \cdot x = \lambda x$ combine to give

$$(I - M) \cdot y + (I - M) \cdot z = \lambda y + \lambda z.$$

In view of $(**)$, we must have

$$(I - M) \cdot y = \lambda z \quad \text{and} \quad (I - M) \cdot z = \lambda y.$$

If we rewrite these identities and use $(*)$, then we have

$$y - \lambda z = M \cdot y \in V_{\tau_1}$$
$$z - \lambda y = M \cdot z \in V_{\tau_2}.$$

The next property will play an important role in §29-4. Since τ_1 and τ_2 map P to itself, it follows that the Coxeter element $\omega = \tau_1\tau_2$ also leaves P invariant.

Lemma C *The order of ω on P = the order of ω on $\mathbb{R}^\ell$.*

Proof The fundamental system $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$ determines a fundamental chamber

$$\mathcal{C} = \{t \in \mathbb{R}^\ell \mid (t, \alpha_i) > 0 \; i = 1, \ldots, \ell\}.$$

By §4-5, W acts freely on the chambers of Δ. Consequently, if ω^k fixes any element of $\mathcal{C}$, then $\omega^k = 1$. So, to prove the lemma, it suffices to show

$$P \cap \mathcal{C} \neq \phi.$$

The element $x = y + z$ belongs to P. The expansion

$$x = x_1\widehat{\alpha}_1 + \cdots + x_n\widehat{\alpha}_\ell$$

implies $(x, \alpha_i) = x_i > 0$ for $i = 1, \ldots, \ell$. Consequently, $x \in \mathcal{C}$ as well. ■

Remark: The preceding argument can easily be altered to show that any point on the line between y and z that is distinct from these two points (i.e., any point of the form $v = \alpha y + \beta z$, where $\alpha > 0, \beta > 0, \alpha + \beta = 1$) belongs to the fundamental chamber $\mathcal{C}$.

29-4 The order of Coxeter elements

In this section, we prove Theorem 29-1B. Let $\Delta \subset \mathbb{R}^\ell$ be a root system of rank ℓ and let $W = W(\Delta)$ be its associated reflection group. Throughout this section, we use the notation and results of §29-3. It was shown in §29-3 that we can form a dihedral subgroup

$$D_m = \langle \tau_1, \tau_2 \mid (\tau_1)^2 = (\tau_2)^2 = (\tau_1\tau_2)^m = 1 \rangle$$

of W, where $\omega = \tau_1\tau_2$ is a Coxeter element. We obtain the involutions τ_1 and τ_2 by picking a decomposition

$$\Sigma = \{\alpha_1, \ldots, \alpha_k\} \coprod \{\alpha_{k+1}, \ldots, \alpha_\ell\}$$

of a fundamental system Σ into two sets, each consisting of roots orthogonal to each other and then letting

$$\tau_1 = s_{\alpha_1} \cdots s_{\alpha_k} \quad \text{and} \quad \tau_2 = s_{\alpha_{k+1}} \cdots s_{\alpha_\ell}.$$

There exists a plane

$$P = \mathbb{R}y + \mathbb{R}z$$

on which D_m acts faithfully and as a reflection group (with τ_1 and τ_2 as reflections). So to prove Theorem 29-1B it suffices to determine the order of ω when it acts on P.

Let H_1 and H_2 be the reflecting lines in P of τ_1 and τ_2. Let $\theta =$ the angle between H_1 and H_2. It follows from Lemma 1-4B that $\omega = \tau_1\tau_2$ is a rotation through 2θ. It follows from the discussion in Chapter 1 that the reflection lines of D_m are equally spaced with an angle θ between any two consecutive lines.

So $\theta = \pi/m$, where $m =$ order ω. First of all, we consider how the reflection lines break into orbits under the action of ω. If m is even, there are two orbits and each orbit contains $m/2$ elements. One orbit contains H_1, while the other contains H_2. If m is odd, then there is only one orbit and it contains m elements.

We next establish a number of facts about the relation between the reflection hyperplanes of W (in $\mathbb{R}^\ell$) and the reflection lines of D_m (in P). We shall prove:

(a) Each reflection hyperplane of W, when restricted to P, restricts to one of the reflection lines of D_m;
(b) The number of reflection hyperplanes restricting to a given reflection line only depends on the orbit of the line;
(c) The number of hyperplanes restricting to H_2 is $(\ell - k)$;
(d) The number of hyperplanes restricting to H_1 is k.

These four facts will establish that $m = 2N/\ell$ because, if m is even, then

$$N = (\ell - k)(m/2) + k(m/2) = \ell m/2,$$

whereas if m is odd, then (b), (c), (d) imply that $\ell - k = k$. So $k = \ell/2$. Hence,

$$N = (\ell/2)m = \ell m/2.$$

In proving (a), (b), (c), (d) we shall need two lemmas. First of all, the elements y and z were chosen to satisfy:

Lemma A *$H_1 = \mathbb{R}y$ and $H_2 = \mathbb{R}z$.*

Secondly:

Lemma B *Given $\alpha \in \Delta$, then:*

(i) $(\alpha, y) = 0$ *if and only if* $\alpha = \pm\alpha_i$ *for* $i = 1, \ldots, k$;
(ii) $(\alpha, z) = 0$ *if and only if* $\alpha = \pm\alpha_i$ *for* $i = k+1, \ldots, \ell$.

Proof We shall prove (i). By definition, $y = x_1\widehat{\alpha}_{k+1} + \cdots + x_\ell\widehat{\alpha}_\ell$. Consequently, $(y, \alpha_i) = 0$ for $i = 1, \ldots, k$. Conversely, suppose $\alpha \in \Delta$ satisfies $(y, \alpha) = 0$. We can assume α is a positive root with respect to $\{\alpha_1, \ldots, \alpha_\ell\}$. Suppose $\alpha = c_1\alpha_1 + \cdots + c_\ell\alpha_\ell$, where $c_i \geq 0$ for $i = 1, \ldots, \ell$. Then $x_1c_1 + \cdots + x_kc_k = (y, \alpha) = 0$. Since $x_i > 0$ for $i = k+1, \ldots, \ell$ we must have $c_{k+1} = \cdots = c_\ell = 0$. Thus α is a linear combination of $\{\alpha_1, \ldots, \alpha_k\}$. Since $\alpha_1, \ldots, \alpha_k$ are mutually orthogonal, the subroot system of Δ generated by them consists of $\{\pm\alpha_k, \ldots, \pm\alpha_k\}$. Consequently, α is one of these elements. ■

Both (c) and (d) are trivial consequences of Lemma B. Also, the transitivity of the action of ω on an orbit forces (b). Regarding (a), first of all, it follows from Lemma B that any hyperplane restricts to a line in P, since $\dim H = \ell - 1$ and $\dim P = 2$ implies that $H \cap P$ is either a line, or all of P. But Lemma B says that y and z cannot both lie on H. Secondly, the line $H \cap P$ is actually one of the reflection lines of D_m, since the transitivity of the action of ω on the chambers of P shows that $H \cap P$ can be moved between the lines H_1 and H_2. If $H \cap P$ does not agree with H_1 or H_2, then, in view of Lemma A, H must contain a point on the line between y and z distinct from those two points. However, by the remark following Lemma C in §29-3, this is not possible.

29-5 Centralizers of Coxeter elements

In this section and the next, we prove some properties of Coxeter elements that will be needed in §32-4, when we further study Coxeter elements in the context of regular elements. The properties are established by using the machinery introduced in §29-3 and §29-4. So this seems the appropriate moment to prove them. Recall that, for any group G and any $\varphi \in W$, we define the centralizer of φ by

$$Z(\varphi) = \{\tau \in G \mid \tau\varphi = \varphi\tau\}.$$

In this section, we prove, except for one fact that will not be verified until §32-4 (see assertion (ii), below), that the centralizers of Coxeter elements are as small as possible. We shall show:

Theorem *Let $W \subset O(\mathbb{E})$ be an irreducible finite reflection group, and let ω be a Coxeter element in W. Then $Z(\omega) = \{\omega^i\}$.*

The rest of the section will be devoted to the proof of this theorem. Let us summarize some facts established in the previous sections. Let $W \subset O(\mathbb{E})$ be an irreducible finite Euclidean reflection group of rank $\ell \geq 2$. It was shown in §29-3 that we can form a dihedral subgroup

$$D_m = \langle \tau_1, \tau_2 \mid (\tau_1)^2 = (\tau_2)^2 = (\tau_1\tau_2)^m = 1 \rangle$$

of W, where $\omega = \tau_1\tau_2$ is a Coxeter element. It was explained in §29-4 how to locate a plane $P \subset \mathbb{E}$ on which D_m acts faithfully as a reflection group, with τ_1 and τ_2 being reflections. Also, ω acts on the plane P as a rotation through the angle $2\pi/h$, where $h = 2N/\ell$, the Coxeter number of W.

There is a close connection between the reflecting hyperplanes and chambers (in $\mathbb{E}$) of W and the reflecting lines and chambers (in P) of D_m. Each reflecting hyperplane of W, when restricted to P, restricts to one of the reflecting lines of D_m. So each chamber of W, when restricted to P, is either the empty set or restricts to a chamber of D_m. In particular, each chamber of D_m can be regarded as the restriction to P of an appropriate chamber of W. This W chamber need not be unique.

If we pass to the complex numbers, we can find $x \in P \otimes \mathbb{C}$ such that

$$\omega \cdot x = \xi x,$$

where ξ is an h-th root of unity. We need one fact about x and one fact about ξ.

(i) $\{x, \bar{x}\}$ is a $\mathbb{C}$ basis of $P \otimes \mathbb{C}$.

First of all, $h \geq 3$ because $h = 2$ leads to a contradiction. By Theorem 29-1B, $h = 2$ implies that $N = \ell$. Consequently, if $\{\alpha_1, \ldots, \alpha_\ell\}$ is a fundamental system of a root system of Δ, then we must have $\Delta = \{\pm\alpha_1, \ldots, \pm\alpha_\ell\}$. However, we are assuming that W, and hence Δ, is both irreducible and of rank ≥ 2. On the other hand, this Δ is only irreducible if $\ell = 1$.

We now know that ω is a rotation of P of order $h \geq 3$. The eigenvectors of such a rotation are not real. So $x = a + bi$, where $a, b \in P$ are independent. Thus $\{x, \bar{x}\}$ is a $\mathbb{C}$ basis of $P \otimes \mathbb{C}$.

(ii) The multiplicity of ξ as an eigenvalue of ω is one.

This fact will be assumed, and will be verified by future arguments. In Theorem 32-2B, we shall reduce the eigenvalue data of Coxeter elements to facts about invariant theory. In particular, it will follow that assertion (ii) is a consequence of Proposition 22-6. See the Remark at the end of §32-2 for further discussion.

Now pick $\tau \in Z(\omega)$. To prove the theorem, it suffices to show that $\tau \in D_m$, since it is easy to see that the only elements from $D_m = \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ commuting with $\omega \in \mathbb{Z}/m\mathbb{Z}$ are the powers of ω. The next two lemmas will establish that $\tau \in D_m$.

Lemma A *τ maps P to itself.*

Proof First of all, $\omega(\tau \cdot x) = \tau\omega \cdot x = \xi(\tau \cdot x)$. It now follows from (i) above that

$$\tau \cdot x = \lambda x \quad \text{for some } \lambda \in \mathbb{C}.$$

Therefore,

$$\tau \cdot \bar{x} = \bar{\lambda}\bar{x}$$

as well. Since $\{x, \bar{x}\}$ is a basis of $P \otimes \mathbb{C}$, it follows that τ maps $P \otimes \mathbb{C}$ to itself. Therefore, $P = (P \otimes \mathbb{C}) \cap \mathbb{E}$ is also mapped to itself. ■

Lemma B $\tau \in D_m$.

Proof Since τ permutes the chambers of W and also maps P to itself, it follows that it permutes the chambers of D_m. Let $\mathcal{C}_o$ be a chamber of D_m. Then $\tau \cdot \mathcal{C}_o$ is also a chamber of D_m. Since D_m acts transitively on its chambers, there exists $\varphi \in D_m$ such that

$$\varphi \cdot (\tau \cdot \mathcal{C}_o) = \mathcal{C}_o.$$

Pick a chamber $\widehat{\mathcal{C}_o}$ of W such that $P \cap \widehat{\mathcal{C}_o} = \mathcal{C}_o$. Then $(\varphi\tau) \cdot \widehat{\mathcal{C}_o} \cap \widehat{\mathcal{C}_o} \neq \varnothing$. Since W acts transitively on its chambers this, in turn, forces

$$(\varphi\tau) \cdot \widehat{\mathcal{C}_o} = \widehat{\mathcal{C}_o}.$$

Since W also acts freely on its chambers, this forces $\varphi\tau = 1$. So $\tau = \varphi^{-1} \in D_m$. ■

29-6 Regular elements

Regular elements will be studied in detail in Chapters 32 and 34 in the context of invariant theory. However, we shall introduce the concept of regular elements at this point, since Coxeter elements are regular and the proof of this fact depends on the machinery introduced in §29-3 and §29-4. So, as with the results of the previous section, this seems the appropriate moment to produce this proof. We shall also show that elements of greatest length are regular.

To define regularity, we have to pass from $\mathbb{R}$ to $\mathbb{C}$. Suppose W is acting on $V = \mathbb{R}^\ell$ as a reflection group. The action of W extends to an action on $V_{\mathbb{C}} = \mathbb{C}^\ell$. The W-invariant inner product on V extends to a W-invariant (Hermitian) positive definite form on $V_{\mathbb{C}}$ by the rule

$$(\lambda x, \mu y) = \lambda\bar{\mu}(x, y) \quad \text{for any } \lambda, \mu \in \mathbb{C},\ x, y \in V.$$

The advantage of passing to $\mathbb{C}$ is that all elements of W now have eigenvectors. Each reflecting hyperplane $H_\alpha \subset V$ of W determines a hyperplane $H_\alpha \otimes_{\mathbb{R}} \mathbb{C} \subset V_{\mathbb{C}}$.

Definition: $x \in V_{\mathbb{C}}$ is *regular* if $x \notin \bigcup_\alpha H_\alpha \otimes_{\mathbb{R}} \mathbb{C}$.

Definition: $\varphi \in W$ is said to be *regular* if φ has a regular eigenvector in $V_{\mathbb{C}}$.

In all that follows, let $W = W(\Delta)$ be an irreducible Euclidean reflection group with root system Δ. Let $\Sigma = \{\alpha_1, \ldots, \alpha_\ell\}$ be a fundamental system for Δ, let

$$\Delta = \Delta^+ \coprod \Delta^-$$

be the decomposition of Δ into positive and negative roots of Σ and let

$$\mathcal{C}_o = \{x \in \mathbb{E} \mid (\alpha, x) > 0 \text{ for } \alpha > 0\}$$

be the fundamental chamber determined by Σ.

Examples:

(a) Elements of Greatest Length The element ω_Σ of greatest length with respect to Σ, as defined in §27-1, is regular. We can produce an explicit regular eigenvalue for ω_Σ. Let

$$\rho = \sum_{\alpha > 0} \alpha.$$

This element has already been studied in §13-2. First of all, since $\omega_\Sigma \cdot \Sigma = -\Sigma$, it follows that $\omega_\Sigma \cdot \Delta^+ = \Delta^-$ and, so, $\omega_\Sigma \cdot \rho = -\rho$. On the other hand, ρ is regular. For it was demonstrated in the proof of Lemma 13-2B that $\rho \in \mathcal{C}_o$.

(b) Coxeter Elements The Coxeter element $\omega = s_{\alpha_1} \cdots s_{\alpha_\ell}$ associated with Σ is regular. It was shown in §29-3 that we can choose a plane $P \subset \mathbb{R}^\ell$ so that ω acts on the plane P as a rotation through the angle $2\pi/h$, where $h =$ the order of ω as an element of the group $W(\Delta)$. If we pass to the complex numbers, we can find $x \in P \otimes \mathbb{C}$ such that

$$\omega \cdot x = e^{2\pi i/h} x.$$

It was pointed out in §29-5 that, since the eigenvectors of a rotation are not real, $\{x, \bar{x}\}$ is a $\mathbb{C}$ basis of $P \otimes \mathbb{C}$. It follows that x is regular. For, suppose $(x, \alpha) = 0$ for some $\alpha \in \Delta$. Then $(\bar{x}, \alpha) = \overline{(x, \alpha)} = 0$ as well. (Here we have used the fact that α is real, so $\alpha = \bar{\alpha}$.) Since $\{x, \bar{x}\}$ is a basis of $P \otimes \mathbb{C}$, we know that $(t, \alpha) = 0$ for all $t \in P$. But, by the remark following Lemma 29-3C, P contains elements from the fundamental chamber $\mathcal{C}_0$. So we have a contradiction.

30 Minimal decompositions

During the study of finite reflection groups in the first eight chapters of the book, we analyzed, in great depth, how elements of W can be decomposed using fundamental reflections. In this chapter, we take a slightly different approach based on the work of Carter [2]. We shall study decompositions of elements of W involving arbitrary reflections from W. These decompositions have the double advantage of being simpler and still containing valuable information.

30-1 Main results

Let $W \subset O(\mathbb{E})$ be an finite reflection group with associated root system $\Delta \subset \mathbb{E}$. Let

$$R = \{s_\alpha \mid \alpha \in \Delta\}$$

be the set of reflections in W. Since W is generated by reflections, every $\varphi \in W$ has at least one decomposition $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$ in terms of the elements of R. A decomposition $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$ where k is as small as possible will be called a *minimal decomposition* (or *minimal expression*) for φ, and k will be called the *minimal length*, $L(\varphi)$, of φ. So:

Definition: $L(\varphi) =$ the minimal k such that $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$, where $\{s_{\alpha_1}, \ldots, s_{\alpha_k}\}$ is a set of reflections in W (repetitions allowed).

If we compare this definition of length with that from Chapter 4, in which we decomposed elements of W using only fundamental reflections, then the two concepts are related via the inequality

$$L(\varphi) \leq \min_{\Sigma}\{\ell(\varphi)\},$$

where, in the right-hand side, $\ell(\varphi)$ ranges over length with respect to every fundamental system Σ of the root system Δ. In general, this is a strict inequality. See the example at the end of this section.

The main goal of this chapter is to provide some interesting characterizations of minimal length and minimal decompositions. Given $\varphi \in W$, let

$$\mathbb{E}^\varphi = \text{the elements of } \mathbb{E} \text{ fixed by } \varphi$$

$$\mathbb{E}_\varphi = \text{the orthogonal complement of } \mathbb{E}^\varphi.$$

If φ is an involution, then $\mathbb{E}_\varphi$ and $\mathbb{E}^\varphi$ are the ± 1 eigenspaces defined in §27-1. In general, φ acts on $\mathbb{E}_\varphi$ with no fixed points. And, if we pass to the compex numbers (so that φ is diagonalizable), then $\mathbb{E}_\varphi \otimes_{\mathbb{R}} \mathbb{C}$ is spanned by eigenvectors corresponding to eigenvalues $\zeta \neq 1$. The subspaces $\mathbb{E}_\varphi$ and $\mathbb{E}^\varphi$ are related to minimal decompositions of φ.

Proposition A *If $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$ is a minimal expression for φ, then*

(i) $\mathbb{E}^\varphi = \bigcap_{i=1}^k H_{\alpha_i}$;

(ii) $\mathbb{E}_\varphi =$ *the subspace spanned by* $\{\alpha_1, \dots, \alpha_k\}$.

Proposition B $L(\varphi) = \dim \mathbb{E}_\varphi$.

Using these facts, we can obtain the following characterizations of minimal decompositions.

Theorem A *Given* $\varphi \in W$, *then* $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$ *is a minimal expression for* φ *if and only if* $\{\alpha_1, \dots, \alpha_k\}$ *are linearly independent.*

Theorem B *Given an involution* $\tau \in W$, *then* $\tau = s_{\alpha_1} \cdots s_{\alpha_k}$ *is a minimal expression for* τ *if and only if* $\{\alpha_1, \dots, \alpha_k\}$ *are orthogonal.*

Minimal decompositions have other important features, which are summarized in the following remarks.

Remark 1: We can represent a minimal decomposition $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$ by a graph. We can associate a graph to the vectors $\{\alpha_1, \dots, \alpha_k\}$ using the same conventions as were employed in §8-6 to associate the Coxeter graph to a fundamental system of a reflection group. If the graph contains no cycles (i.e., is a tree), then it is representing the Coxeter element of a reflection subgroup of W. But graphs with cycles do exist. See Carter [2] for examples of such graphs.

Remark 2: There is a further restriction on minimal decompositions. For every φ, we can find a minimal decomposition

$$\varphi = s_{\alpha_1} \cdots s_{\alpha_k} s_{\alpha_{k+1}} \cdots s_{\alpha_{k+m}},$$

where both $\{\alpha_1, \dots, \alpha_k\}$ and $\{\alpha_{k+1}, \dots, \alpha_{k+m}\}$ are sets whose elements are pairwise orthogonal. Equivalently, every element can be decomposed as a product $\varphi = \tau_1 \tau_2$ of two involutions. Recall that in §29-3 such a decomposition was established in the case of Coxeter elements. Unfortunately, the proof of this fact for an arbitrary conjugacy class still depends on a case-by-case analysis of the irreducible reflection groups. The arguments are due to Carter (Weyl group case) and Springer (non-Weyl case). See Carter [2] and Springer [2]. Carter used this strengthened version of a minimal decomposition to classify the conjugacy classes of the crystallographic reflection groups.

We close this section with an example illustrating that the inequality $L(\varphi) \leq \min_\Sigma \{\ell(\varphi)\}$ is, in general, a strict inequality.

Example: The dihedral groups D_m were shown in §1-4 to be reflection groups in the plane. We have $L(\rho) \leq 2$ for each $\rho \in D_m$, since it was shown in §1-4 that each element from the group acts on the plane as either a reflection ($\det = -1$) or a rotation ($\det = 1$). Then we have

$$L(\rho) = \begin{cases} 1 & \text{if } \rho \text{ is a reflection} \\ 2 & \text{if } \rho \text{ is a rotation.} \end{cases}$$

Let ρ be any rotation in D_m. If we pick a reflection $s \in D_m$, then $s' = \rho s$ is a reflection as well because $\det(\rho s) = \det(\rho)\det(s) = (1)(-1) = -1$. And we can rewrite the identity $s' = \rho s$ as $\rho = s's$.

On the other hand, the presentation

$$D_m = \langle s_1, s_2 \mid (s_1)^2 = (s_2)^2 = (s_1 s_2)^m = 1 \rangle$$

tells us that $\ell(\rho) = 2$ with respect to the fundamental reflection $\{s_1, s_2\}$ only when $\rho = s_1 s_2$ or $\rho = s_2 s_1$. In particular, ρ must be a rotation of order m. So if $\rho \neq 1$ is a rotation of order $< m$, then $\ell(\rho) > 2$ for any choice of fundamental reflections $\{s_1, s_2\}$.

30-2 The proof of Propositions 30-1A and 30-1B

We begin with a number of definitions. We shall make use of certain subspaces arising out of any fixed decomposition $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$ (minimal or not). Given such a decomposition, let

$$H = \text{the subspace spanned by } \{\alpha_1, \ldots, \alpha_k\}.$$

The orthogonal complement of H is given by

$$H^{\perp} = \bigcap_{i=1}^{k} H_{\alpha_i}.$$

We have already defined (in §30-1) the subspaces $\mathbb{E}^{\varphi}$ and $\mathbb{E}_{\varphi}$. We have $H^{\perp} \subset \mathbb{E}^{\varphi}$. Since $\mathbb{E}^{\varphi}$ and $\mathbb{E}_{\varphi}$ are orthogonal, we also have $\mathbb{E}_{\varphi} \subset H$. Moreover, $H^{\perp} = \mathbb{E}^{\varphi}$ if and only if $\mathbb{E}_{\varphi} = H$.

We also have need of certain subgroups of W. Given $\varphi \in W$, let

$$W_{\varphi} = \text{the isotropy subgroup of } W \text{ which fixes } \mathbb{E}^{\varphi}.$$

In particular, $\varphi \in W_{\varphi}$. Being an isotropy group, W_{φ} is a parabolic subgroup and, hence, generated by reflections (see §5-2). Recall that the rank of a reflection group is the rank of the underlying root system. Let

$$\ell = \operatorname{rank} W = \operatorname{rank} \Delta.$$

If $\mathbb{E}^{\varphi} \neq 0$, then, as was observed in the remark following Proposition 5-2A, W_{φ} is a reflection subgroup of rank $< \ell$. Such a fact is useful in making inductive arguments. A more precise restriction on rank is that

$$\operatorname{rank} W_{\varphi} \leq \dim \mathbb{E}_{\varphi}.$$

To prove this inequality, it suffices to show that the root system of the reflection group W_{φ} lies in $\mathbb{E}_{\varphi}$. Since W_{φ} acts trivially on $\mathbb{E}^{\varphi}$, we have $\mathbb{E}^{\varphi} \subset H_{\alpha}$ for each reflection $s_{\alpha} \in W_{\varphi}$. So α is orthogonal to $\mathbb{E}^{\varphi}$, i.e., $\alpha \in \mathbb{E}_{\varphi}$.

Lemma $L(\varphi) \leq \ell$.

Proof We proceed by induction on rank. First of all, by induction, we can assume

$$\mathbb{E}^{\varphi} = 0$$

because $\varphi \in W_{\varphi}$ and, by our previous remarks, W_{φ} has smaller rank than W whenever $\mathbb{E}^{\varphi} \neq 0$. Secondly, pick $\alpha \in \Delta$. It suffices to show that φs_{α} can be decomposed using at most $\ell - 1$ reflections. We are now assuming that $\varphi - 1$ is nonsingular. So we can pick $x \in \mathbb{E}$ such that $(\varphi - 1) \cdot x = \alpha$. In other words,

$$\varphi \cdot x = x + \alpha.$$

It is then also true that

$$s_{\alpha} \cdot x = x + \alpha$$

because $(x, x) = (\varphi \cdot x, \varphi \cdot x) = (x + \alpha, x + \alpha) = (x, x) + 2(x, \alpha) + (\alpha, \alpha)$. Thus $2(\alpha, x)/(\alpha, \alpha) = -1$. Substitute this identity into formula (A-1) of §1-1.

It follows from the above identities that $\varphi \cdot x = s_{\alpha} \cdot x$, i.e.,

$$(\varphi s_{\alpha}) \cdot x = x.$$

So $\varphi s_{\alpha} \in W_x$. But, again, the isotropy group W_x has rank $< \ell$. So, by induction on rank, φs_{α} can be decomposed using $\leq \ell - 1$ reflections. ∎

Proof of Proposition 30-1B First of all,

$$\dim \mathbb{E}_{\varphi} \leq L(\varphi).$$

For, if $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$, then the inclusion $\mathbb{E}_{\varphi} \subset H$ tells us that $\dim \mathbb{E}_{\varphi} \leq \dim H \leq k$. Secondly,

$$L(\varphi) \leq \dim \mathbb{E}_{\varphi}$$

because $\varphi \in W_{\varphi}$ and, as noted above, $\operatorname{rank} W_{\varphi} \leq \dim \mathbb{E}_{\varphi}$. We now appeal to the above lemma. ∎

Proof of Proposition 30-1A Given a decomposition $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$, the inclusion

$$\mathbb{E}_{\varphi} \subset H$$

with the inequalities

$$L(\varphi) \leq \dim \mathbb{E}_{\varphi} \leq \dim H \leq k$$

force $\mathbb{E}_{\varphi} = H$ whenever $L(\varphi) = k$, i.e., whenever the decomposition is minimal. By orthogonality, we also have the equality $\mathbb{E}^{\varphi} = H^{\perp}$. ∎

30-3 The proof of Theorem 30-1A

First of all, if $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$ is a minimal decomposition of φ, then, by Proposition 30-1A, $\mathbb{E}_\varphi$ is spanned by $\{\alpha_1, \ldots, \alpha_k\}$ while, by Proposition 30-1B, $\dim \mathbb{E}_\varphi = L(\varphi) = k$. It follows that $\{\alpha_1, \ldots, \alpha_k\}$ is independent.

The converse, namely that $\{\alpha_1, \ldots, \alpha_k\}$ independent forces $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$ to be a minimal expression, requires more work. *Let $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$ be any decomposition of φ.* The rest of this section will be devoted to proving:

Proposition *If $\{\alpha_1, \ldots, \alpha_k\}$ are independent, then* $\dim \mathbb{E}_\varphi = k$.

This proposition implies that $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$ is minimal whenever $\{\alpha_1, \ldots, \alpha_k\}$ is independent, since we know from Proposition 30-1B that $\dim \mathbb{E}_\varphi = L(\varphi)$. Consequently, if $\dim \mathbb{E}_\varphi = k$, then $L(\varphi) = k$.

As the first step in proving the proposition, we point out the following easy consequence of formula (A-1) in §1-1.

Lemma A *For all $x \in \mathbb{E}$, $\varphi \cdot x = x + y$, where y is a linear combination of $\{\alpha_1, \ldots, \alpha_k\}$.*

Next, as in §30-2, let

$$H = \text{the subspace spanned by } \{\alpha_1, \ldots, \alpha_k\}.$$

The independence hypothesis implies that $\dim H = k$. By the above lemma, $\varphi = s_{\alpha_1} \cdots s_{\alpha_k}$ maps H to itself. We want to show that

$$H^\varphi = \{0\}.$$

For, the inclusion $\mathbb{E}_\varphi \subset H$ can be strengthened to $H = H^\varphi \oplus \mathbb{E}_\varphi$.

We proceed by induction on k. The case $k = 2$ was dealt with in §1-4. We showed that $s_{\alpha_1} s_{\alpha_2}$ acts on the plane $P = \mathbb{R}\alpha_1 + \mathbb{R}\alpha_2$ as a rotation through twice the angle between α_1 and α_2. Assume that the lemma is true for the $k - 1$ case. Let

$$H_0 = \text{the hyperplane spanned by } \{\alpha_2, \ldots, \alpha_k\}.$$

More generally, pick $0 \neq \beta \in H$ which is orthogonal to H_0 and, for each $t \in \mathbb{R}$, let

$$H_t = \text{the affine hyperplane } \beta_t + H_0$$

where $\beta_t = t\beta$. These parallel hyperplanes $\{H_t\}$ provide a decomposition of H. The action of φ on H does not necessarily respect this decomposition. Nevertheless, for each H_t, we can consider

$$H_t^\varphi = \text{the elements of } H_t \text{ fixed by } \varphi.$$

To prove the proposition it suffices to show:

Lemma B $H_0^\varphi = \{0\}$.

Lemma C $H_t^\varphi = \varnothing$ *if $t \neq 0$.*

We use the induction hypothesis to prove these facts. The induction hypothesis will be introduced via the decomposition

$$\varphi = s_\alpha \varphi_0,$$

where

$$\varphi_0 = s_{\alpha_2} \cdots s_{\alpha_k}$$

and where, for convenience, we have let $\alpha = \alpha_1$. By Lemma C, φ_0 maps H_0 to itself. The induction hypothesis implies that

$$H_0^{\varphi_0} = \{0\}.$$

Observe also that, by formula (A-1) of §1-1,

$$\varphi_0 \cdot \beta_t = \beta_t$$

because β_t is orthogonal to $\{\alpha_2, \ldots, \alpha_k\}$.

Proof of Lemma B Clearly, 0 is a fixed point of φ. Consider the decomposition $\varphi = s_\alpha \varphi_0$. As observed above, $H_0^{\varphi_0} = \{0\}$. Pick $0 \neq x \in H_0$ and let $y = \varphi_0 \cdot x$. Then $y \in H_0$ and $y \neq x$. We break the proof into two cases.

(i) $y \in H_\alpha$: Then $s_\alpha \cdot y = y$. So $\varphi \cdot x = s_\alpha \cdot y = y \neq x$;
(ii) $y \notin H_\alpha$: In other words, $(\alpha, y) \neq 0$. Then we can write

$$s_\alpha \cdot y = y + c\alpha,$$

where $c = 2(\alpha, y)/(\alpha, \alpha) \neq 0$. This forces $s_\alpha \cdot y \notin H_0$. For, otherwise, $\alpha = (1/c)(y - s_\alpha \cdot y) \in H_0$, which contradicts the independence of $\{\alpha_1, \ldots, \alpha_k\}$. Clearly, if $\varphi \cdot x = s_\alpha \cdot y \notin H_0$, then $\varphi \cdot x \neq x$. ■

Proof of Lemma C Assume that $t \neq 0$. Every element of $H_t = \beta_t + H_0$ can be written uniquely as $\beta_t + x$, where $x \in H_0$. We want to show that $\varphi \cdot (\beta_t + x) = \beta_t + x$ is impossible.

The Case $x = 0$ First of all, we deal with the case $x = 0$. In this case, the equality $\varphi \cdot (\beta_t + x) = \beta_t + x$ reduces to

$$s_\alpha \cdot \beta_t = \beta_t.$$

But then $\alpha = \alpha_1$ and β are orthogonal. So $\alpha_1 \in H_0$, which contradicts the independence of $\{\alpha_1, \ldots, \alpha_\ell\}$.

The Case $x \neq 0$ Now consider $x \neq 0$. We can write

$$\varphi_0 \cdot (\beta_t + x) = \beta_t + y, \quad \text{where } y = \varphi_0 \cdot x \in H_0.$$

Thus

$$\varphi \cdot (\beta_t + x) = s_\alpha \cdot (\beta_t + y) = (\beta_t + y) + c\alpha \quad \text{for some } c \in \mathbb{R}.$$

The equality $\varphi \cdot (\beta_t + x) = \beta_t + x$ then forces the identity

$$\beta_t + x = \beta_t + y + c\alpha.$$

If $c \neq 0$, this forces $\alpha = (1/2)(x - y) \in H_0$, which contradicts the independence of $\{\alpha_1, \ldots, \alpha_k\}$. If $c = 0$, this forces $x = y$. Since $x \neq 0$, this is impossible by the argument in $(*)$. ■

30-4 The proof of Theorem 30-1B

In this section, we prove Theorem 30-1B. Let $\Delta \subset \mathbb{E}$ be a root system with associated reflection group $W \subset O(\mathbb{E})$. Let $\tau = s_{\alpha_1} \cdots s_{\alpha_k}$ be a decomposition of an involution τ. One implication of Theorem 30-1B follows from Theorem 30-1A, since if $\{\alpha_1, \ldots, \alpha_k\}$ are orthogonal, then they are independent and so, by Theorem 30-1A, the decomposition $\tau = s_{\alpha_1} \cdots s_{\alpha_k}$ is minimal.

Conversely, assume that the decomposition $\tau = s_{\alpha_1} \cdots s_{\alpha_k}$ is minimal. It follows from Proposition 30-1B that $\{\alpha_1, \ldots, \alpha_k\}$ is a basis of the eigenvalue space $\mathbb{E}_\tau$. We want to prove that $\{\alpha_1, \ldots, \alpha_k\}$ are orthogonal. The approach is to show that, for each $1 \leq i \leq \ell$

$(*)$ $\qquad \{\alpha_1, \ldots, \alpha_i\}$ are orthogonal to $\{\alpha_{i+1}, \ldots, \alpha_\ell\}$.

We begin by showing

$$\alpha_1 \text{ is orthogonal to } \{\alpha_2, \ldots, \alpha_\ell\}.$$

It suffices to show that every $x \in H_{\alpha_1} \cap \mathbb{E}_\tau$ can be expanded in terms of $\{\alpha_2, \ldots, \alpha_\ell\}$. For, since $\dim H_{\alpha_1} \cap \mathbb{E}_\tau = k - 1$, this forces $\{\alpha_2, \ldots, \alpha_k\}$ to be a basis of H_{α_1}.

Since $x \in \mathbb{E}_\tau$, we have

$$(s_{\alpha_1} \cdots s_{\alpha_\ell}) \cdot x = \tau \cdot x = -x.$$

Since $x \in \mathbb{E}_\tau$, it follows that

$$(s_{\alpha_2} \cdots s_{\alpha_\ell}) \cdot x = -s_{\alpha_1} \cdot x = -x.$$

Hence,

$$2x = x - (s_{\alpha_2} \cdots s_{\alpha_\ell}) \cdot x.$$

By Lemma 30-3A, the right-hand side of this identity can be expanded in terms of $\{\alpha_2, \ldots, \alpha_\ell\}$. Passing to the left-hand side of the identity, x can also be expanded in terms of $\{\alpha_2, \ldots, \alpha_\ell\}$ as well.

Regarding the proof of $(*)$, it suffices to show that every $x \in H_{\alpha_1} \cap \cdots \cap H_{\alpha_i} \cap \mathbb{E}_\tau$ can be expanded in terms of $\{\alpha_{i+1}, \ldots, \alpha_\ell\}$. We do this by generalizing the argument above and, in particular, deriving the formula

$$2x = x - (s_{\alpha_{i+1}} \cdots s_{\alpha_\ell}) \cdot x.$$

IX Eigenvalues

The main theme in our discussion of invariant theory has been that the associated ring of invariants of a pseudo-reflection group provides a great deal of information about the structure of the group. The last four chapters of the book provide further demonstrations of this fact. These chapters discuss how invariant theory can be used to analyze the eigenvalues of elements from pseudo-reflection groups. This information is used, in turn, to obtain a limited amount of information about conjugacy classes of elements and subgroups. Most of the results of these four chapters are due to Solomon and Springer.

In Chapter 31, we use Solomon's theorem from Chapter 22 to obtain data about the occurrence of eigenvalues for arbitrary elements of pseudo-reflection groups. In Chapter 32, we introduce regular elements and study their eigenvalues. In Chapter 33, we place invariant rings in the context of algebraic geometry. We show that we can view the ring of invariants of $G \subset GL(V)$ as the coordinate ring of the orbit space V/G. In Chapter 34, we use this fact to obtain additional results about the eigenspaces of elements of G. In particular, we obtain information about how eigenspaces for elements of G are related through the action of G. We can use this information to obtain information about conjugacy classes in G. We also demonstrate that centralizers of regular elements act on eigenspaces as pseudo-reflection groups.

31 Eigenvalues for reflection groups

The most fundamental question we can ask about the invariant theory of a pseudo-reflection group is how to calculate its degrees and exponents. In this chapter, we explain how to characterize exponents in terms of data about the eigenvalues of elements from the group. The relation given in its full generality is due to Pianzola-Weiss [1]. Their result is an extension of the fundamental work of Shephard-Todd [1] and Solomon [1].

31-1 Eigenspaces and exponents

Let V be a finite dimensional vector space over a field $\mathbb{F}$ and let $G \subset \mathrm{GL}(V)$ be a *finite nonmodular pseudo-reflection group.* In Chapter 18, we defined the degrees $\{d_1, \ldots, d_n\}$ and the exponents $\{m_1, \ldots, m_n\}$ of G. Recall that they are related by the rule $m_i = d_i - 1$. For any $\varphi \in G$, we can speak of its invariant subspace V^{φ}. These are the elements of V fixed by φ. Let

$$h_i = \text{the number of elements in } G \text{ with invariant subspace of dimension } i.$$

The numbers $\{h_0, h_1, \ldots, h_n\}$ are related to the exponents of G by the following identity.

***Theorem A* (Solomon)** $\prod_{i=1}^n (T + m_i) = h_0 + h_1 T + \cdots + h_n T^n$.

This identity was established in Shephard-Todd [1] for the case $\mathbb{F} = \mathbb{C}$ and in Solomon [1] for the case $\operatorname{char} \mathbb{F} = 0$. We can view the Solomon relation as a generalization of several facts established in Chapter 18. It was shown there that

(i) $|G| = \prod_{i=1}^n d_i$;
(ii) number of pseudo-reflections in $G = m_1 + \cdots + m_n$.

These facts are easy consequences of the identity in the theorem. Regarding (a), let $T = 1$. Regarding (b), compare the coefficients of T^{n-1}.

A more comprehensive, and complicated, result than Theorem A has been obtained in Pianzola-Weiss [1]. Let $d \geq 2$ be a positive integer and suppose that $\mathbb{F}$ contains a primitive d-th root of unity, denoted ξ. For any $\varphi \in G$, let

$$V(\varphi, \xi) = \{x \in V \mid \varphi \cdot x = \xi x\}$$

the eigenspace corresponding to ξ. Let

$$h_i(\xi) = \text{the number of elements in } G \text{ where } \dim V(\varphi, \xi) = i.$$

The above Solomon relation can be generalized to an identity involving these numbers. Let

$$\pi(d) = \prod_{d_i \not\equiv 0 \ (\mathrm{mod}\ d)} d_i$$

$$P_d(T) = \prod_{d_i \equiv 0 \ (\mathrm{mod}\ d)} (T + m_i).$$

Theorem B **(Pianzola-Weiss)** *Suppose that $\mathbb{F}$ contains ξ, a primitive d-th root of unity. Then*

$$\pi(d)P_d(T) = h_0(\xi) + h_1(\xi)T + \cdots + h_n(\xi)T^n.$$

These theorems provide a way of counting the number of elements in G having eigenvalues with certain multiplicities. Such results are extremely useful in studying the elements of G. The next two corollaries are concerned with determining when $h_1(\xi) > 0$ and when $h_n(\xi) > 0$ ($n = \dim_{\mathbb{F}} V$).

Corollary A *Suppose that $\mathbb{F}$ contains ξ, a primitive d-th root of unity. Then there exists $\varphi \in G$ having ξ as an eigenvalue if and only if d divides d_i for some i.*

Next, given $\xi \in \mathbb{F}$, let

$$\xi\colon V \to V$$

denote the map that is scalar multiplication by ξ.

Corollary B *Suppose that $\mathbb{F}$ contains ξ, a primitive d-th root of unity. Then the scalar map $\xi \in G$ if and only if d divides d_i for all i.*

Recall that the *exponent* of the group G is defined by

$$e(G) = \min\{d \mid \varphi^d = 1 \text{ for all } \varphi \in G\},$$

whereas the *center* of G is defined by

$$Z(G) = \{\tau \in G \mid \varphi\tau = \tau\varphi \text{ for all } \varphi \in G\}.$$

Corollary C *If $\mathbb{F}$ is algebraically closed and G acts irreducibly on V, then*

(i) $|Z(G)| = g.c.d.\{d_1, \ldots, d_n\}$;
(ii) $e(G) = l.c.m.\{d_1, \ldots, d_n\}$.

Example: Euclidean Reflection Groups

In the case of Euclidean reflection groups, we must have $d = 2$ and $\xi = -1$. The above results reduce to assertions made (but not proved) in §27-2. Corollary B asserts that $-1 \in W$ if and only if each d_i is even. Corollary C (plus Proposition 18-6) asserts that, in the above case, -1 actually generates $Z(W)$ (provided the further hypothesis of the corollary is also satisfied).

We assume that $\mathbb{F}$ is algebraically closed in the above corollary in order to ensure that $\mathbb{F}$ contains the eigenvalues of each elements of G. It then follows from Schur's Lemma in Appendix B that $Z(G)$ consists of the scalar maps $\xi\colon V \to V$ belonging to G. So (i) follows from Corollary B. Regarding (ii), we can deduce from Corollary A that d divides $e(G)$ if and only if d divides d_i for some i.

The proofs of Theorems A and B will be presented in §31-2 and §31-3. Theorem A was first verified by Shephard and Todd [1] for complex reflection groups using a case-by-case argument. The general proof of the theorem given in this chapter is due to Solomon [1]. The proof of Theorem B is a modification of Solomon's proof and is due to Pianzola and Weiss. The proofs are analogous to the

proof given in §18-3 that $|G| = \prod_{i=1}^n d_i$. That proof was an argument involving Poincaré series and, in particular, Molien's theorem. It was based on the fact that $S(V)^G$ is a polynomial algebra and, hence, that its Poincaré series is of the form

$$P_t S(V)^G = \frac{1}{1-t^{d_1}} \cdots \frac{1}{1-t^{d_n}}.$$

By comparing this identity with the expansion of $P_t S(V)^G$ given by Molien's theorem, we obtain $|G| = \prod_{i=1}^n d_i$.

31-2 The proof of Theorem A

The proofs of Theorems A and B are manipulations involving Poincaré series. Let V be a finite dimensional vector space over a field $\mathbb{F}$ and let $G \subset GL(V)$ be *a finite nonmodular pseudo-reflection group*. The identity

$$(*) \qquad \frac{\prod_{i=1}^n (1+YX^{d_i-1})}{\prod_{i=1}^n (1-X^{d_i})} = \frac{1}{|G|} \sum_{\varphi \in G} \frac{\det(1+Y\varphi)}{\det(1-X\varphi)}$$

was established in §22-4 and represents two different expansions of the Poincaré series of the extended ring of invariants $[S(V) \otimes E(V)]^G$. This identity is the key to proving Theorems A and B. We shall manipulate this identity to obtain the identities given in Theorems A and B. Theorem A is actually a special case of Theorem B and its proof is, similarly, a special case of the proof of Theorem B. However, we shall still present the proof of Theorem A, since it will serve as a useful motivation for the more complicated manipulation needed to obtain Theorem B.

The procedure in proving Theorem A is to take identity $(*)$ from above, substitute $Y = -1 + T(1-X)$ on each side, simplify, and then let $X = 1$.

Left-Hand Side If we let $Y = -1 + T(1-X)$, then

$$\begin{aligned} \text{LHS} &= \prod_{i=1}^n [1 - X^{d_i-1} + (1-X)TX^{d_i-1}] \Big/ \left[\prod_{i=1}^n (1-X^{d_i})\right] \\ &= \prod_{i=1}^n [1 + X + \cdots + X^{d_i-2} + TX^{d_i-1}] \Big/ \left[\prod_{i=1}^n (1 + X + \cdots + X^{d_i-1})\right]. \end{aligned}$$

If we let $X = 1$, then

$$\text{LHS} = \prod_{i=1}^n [(d_i - 1) + T] \Big/ \left[\prod_{i=1}^n d_i\right].$$

Right-Hand Side It suffices to consider each of the terms $\frac{\det(1+Y\varphi)}{\det(1-X\varphi)}$ in the RHS separately and show that, if $\dim V^\varphi = k$, then $\frac{\det(1+Y\varphi)}{\det(1-X\varphi)} = T^k$. We shall work in

the algebraic closure $\bar{\mathbb{F}}$ of $\mathbb{F}$. The eigenvalue 1 occurs with multiplicity k. Suppose $\{\omega_1, \ldots, \omega_{n-k}\}$ are the other eigenvalues. Then

$$\frac{\det(1 + Y\varphi)}{\det(1 - X\varphi)} = \frac{(1+Y)^k \prod_{i=1}^{n-k}(1 + \omega_i Y)}{(1-X)^k \prod_{i=1}^{n-k}(1 - \omega_i X)}.$$

If we let $Y = -1 + T(1 - X)$, then

$$\frac{\det(1 + Y\varphi)}{\det(1 - X\varphi)} = T^k \frac{\prod_{i=1}^{n-k}[1 - \omega_i + \omega_i(1 - X)T]}{\prod_{i=1}^{n-k}(1 - \omega_i X)}.$$

Letting $X = 1$, we have

$$\frac{\det(1 + Y\varphi)}{\det(1 - X\varphi)} = T^k.$$

31-3 The proof of Theorem B

This time the recipe is to take identity $(*)$ from §31-2, substitute $Y = -\xi^{-1} + (1 - \xi X)T$ in each side, simplify (most of the time), and then let $X = \xi^{-1}$. These manipulations will lead us to the identity

$$\pi(d) \prod_{d_i \equiv 0 \pmod d} (\xi T + m_i) = h_0(\xi) + h_1(\xi)\xi T + \cdots + h_n(\xi)(\xi T)^n.$$

This is equivalent to the identity given in Theorem B. Just replace ξT by T.

Right-Hand Side We shall show that, if $\dim V(\varphi, \xi) = k$, then $\frac{\det(1+Y\varphi)}{\det(1-X\varphi)} = (\xi T)^k$. The eigenvalue ξ occurs with multiplicity k. Suppose $\{\omega_1, \ldots, \omega_{n-k}\}$ are the other eigenvalues. Then

$$\frac{\det(1 + Y\varphi)}{\det(1 - X\varphi)} = \frac{(1+\xi Y)^k \prod_{i=1}^{n-k}(1 + \omega_i Y)}{(1-\xi X)^k \prod_{i=1}^{n-k}(1 - \omega_i X)}.$$

When we let $Y = -\xi^{-1} + (1 - \xi X)T$, then

$$\frac{\det(1 + Y\varphi)}{\det(1 - X\varphi)} = T^k \frac{\prod_{i=1}^{n-k}\big(1 - \xi^{-1}\omega_i + \omega_i(1 - \xi X)T\big)}{\prod_{i=1}^{n-k}(1 - \omega_i X)}.$$

Letting $X = \xi^{-1}$, we have

$$\frac{\det(1 + Y\varphi)}{\det(1 - X\varphi)} = (\xi T)^k.$$

Left-Hand Side We shall write the LHS in the form $\prod_{i=1}^{n} \frac{1+YX^{d_i-1}}{1-X^{d_i}}$ and consider each factor individually. There are two separate cases to consider.

(i) d does not divide d_i.

The effect of substituting

$$Y = -\xi^{-1} + (1 - \xi X)T$$
$$X = \xi^{-1}$$

is the same as just letting $X = \xi^{-1}$ and $Y = -\xi^{-1}$. In the present case, this gives

$$\frac{1 + YX^{m_i}}{1 - X^{d_i}} = \frac{1 - \xi^{-d_i}}{1 - \xi^{-d_i}} = 1.$$

In particular, the last identity uses the fact that $1 - \xi^{d_i} \neq 0$ (since d does not divide d_i).

(ii) d divides d_i.

In this case, $\xi^{d_i} = 1$ and, so, $\xi^{m_i} = \xi^{-1}$. In particular, the argument from (i) doesn't make sense, since $1 - \xi^{-d_i} = 0$. So a modified argument has to be used. When we let $Y = -\xi^{-1} + (1 - \xi X)$, then

$$\begin{aligned}
\frac{1 + YX^{m_i}}{1 - X^{d_i}} &= \frac{1 - \xi^{-1}X^{m_i} + (1 - \xi X)TX^{m_i}}{1 - X^{d_i}} \\
&= \frac{1 - (\xi X)^{m_i} + (1 - \xi X)TX^{m_i}}{1 - (\xi X)^{d_i}} \\
&= \frac{1 + \xi X + \cdots + \xi X^{m_i - 1} + TX^{m_i}}{1 + \xi X + (\xi X)^2 + \cdots + (\xi X)^{d_i - 1}}.
\end{aligned}$$

Letting $X = \xi^{-1}$, we have

$$\frac{1 + YX^{m_i}}{1 - X^{d_i}} = \frac{m_i + \xi Y}{d_i}.$$

32 Eigenvalues for regular elements

In this chapter, we discuss the eigenvalues of certain special elements of pseudo-reflection groups called regular elements. We shall prove that there are significant relations between such eigenvalues and the exponents of the group. Notably, we shall demonstrate that the exponents can be characterized in terms of the eigenvalue data of regular elements. The results of this chapter are due to Coxeter [2] and Springer [2].

32-1 Regular elements

Throughout this chapter, we shall assume that V is a finite dimensional vector space over a *field* $\mathbb{F}$ *of characteristic zero* and that $G \subset \mathrm{GL}(V)$ *is a finite pseudo-reflection group*. In this chapter, we shall introduce regular elements and establish various eigenvalue properties of these elements. A regular element is defined by the property of possessing a particular type of eigenvector.

Definition: $x \in V$ is *regular* (with respect to G) if it does not lie on the reflecting hyperplane of any pseudo-reflection from G.

Definition: $\varphi \in G$ is regular if it has a regular eigenvector.

Definition: If $\varphi \cdot x = \xi x$ for a regular vector $x \in V$, then $\xi \in \mathbb{F}$ will be called a *regular eigenvalue* of φ.

Example: We have already seen canonical examples of regular elements. It was shown in §29-5 that, if we take an irreducible Euclidean reflection group and work over the complex numbers, then its Coxeter elements are regular. Since the various powers of a regular element are also regular, the powers of Coxeter elements provide additional examples of regular elements. As an explicit example of the complexification of a Coxeter element being regular, we consider the A_ℓ case. Let $V \subset \mathbb{F}^{n+1}$ be the subspace

$$V = \{(x_1, \ldots, x_{n+1}) \mid x_1 + \cdots + x_{n+1} = 0\}.$$

Then Σ_{n+1} acts on V by permuting the coordinates. This action realizes Σ_{n+1} as an n-dimensional pseudo-reflection group. The reflections of Σ_{n+1} are the permutations $\{(i, j) \mid i \leq j\}$. If the field $\mathbb{F}$ contains ξ, a primitive $(n+1)$-st root of unity, then the element

$$\varphi = (1, 2, \ldots, n+1) = (1, 2)(2, 3) \cdots (n, n+1)$$

is regular where a regular eigenvector for φ is

$$x = (\xi^n, \xi^{n-1}, \ldots, \xi, 1).$$

Observe that $\varphi \cdot x = \xi x$. Also, x does not belong to any reflection hyperplane because the permutation (i, j) has reflection hyperplane

$$H_{ij} = \{(x_1, \ldots, x_{n+1}) \mid x_i = x_j\}.$$

So $x \notin H_{ij}$ for any choice of i and j. We conclude that φ is regular.

We record, for future use, some properties of regular vectors and regular elements.

Regular Vectors

We see, by Lemma 30-5A, that V has regular elements provided $\mathbb{F}$ is infinite. Regular vectors have several important properties.

(I-1) Regular vectors are the vectors in V whose isotropy group G_x is trivial.

(I-2) An element of G is determined by its effect on any regular vector of V. Namely, given $\varphi, \tau \in G$, then $\varphi = \tau$ if $\varphi \cdot x = \tau \cdot x$ for any regular $x \in V$. In particular, the order of any $\varphi \in G$ is determined by its effect on x, i.e., if $\varphi^k \cdot x = x$, then $\varphi^k = 1$.

Regarding (I-1), it follows from Corollary 30-1 that the isotropy group G_x is a pseudo-reflection group for every $x \in V$. But, by definition, a regular element of V is one whose isotropy group contains no pseudo-reflections. Regarding (I-2), $\varphi \cdot x = \tau \cdot x$ implies that $\varphi\tau^{-1} \in G_x$. But, as just observed, $G_x = \{1\}$.

Regular Elements

The above facts also have consequences for regular elements. It follows from property (I-2) that

(I-3) If φ is a regular element φ of order d, then φ has a primitive d-th root of unity ξ as a regular eigenvalue.

Suppose that $\varphi \in G$ is regular and $x \in V$ is a regular eigenvector of φ. We can write $\varphi \cdot x = \lambda x$ for some $\lambda \in \mathbb{F}$. Then

$$\varphi^k \cdot x = \lambda^k x \quad \text{for each } k \geq 1.$$

By the argument given above to justify (I-2), $\varphi^k = 1$ if and only if $\lambda^k = 1$.

Property (I-3) can be extended to

(I-4) A regular element φ of order d is diagonalizable. If ξ is any primitive d-th root of unity, then every eigenvalue of φ is of the form ξ^k for some $k \geq 1$.

This is because every eigenvalue of φ is a d-th root of unity (possibly nonprimitive). So if ξ is any fixed primitive d-th root of unity, then any eigenvalue of φ is of the form ξ^k. In particular, it follows from (I-3) that the field $\mathbb{F}$ must contain such a primitive d-th root of unity. Thus $\mathbb{F}$ contains all the eigenvalues of φ and φ is diagonalizable.

Remark 1: It follows from (I-3), and Corollary 31-1A, that the pseudo-reflection group $G \subset \mathrm{GL}(V)$ can have a regular element of order d only if d divides one of the degrees $\{d_1, \ldots, d_n\}$ of G.

Remark 2: It also follows from (I-3) and (I-4) that φ's being regular depends, in part, on the field over which we are working. Given $\varphi \in G$, we have to work in a large enough field to obtain all possible eigenvalues of φ. This consideration clearly arises when we are dealing with Euclidean reflection groups. When discussing regular elements of an Euclidean reflection group $W \subset O(\mathbb{E})$, we pass from $\mathbb{R}$ to $\mathbb{C}$ and consider W acting on $V_{\mathbb{C}} = \mathbb{C}^{\ell}$. The regular elements of W should always be taken to mean the regular elements of the associated complex pseudo-reflection group $W \subset \mathrm{GL}(V_{\mathbb{C}})$.

32-2 Eigenvalues of regular elements

In the rest of this chapter, we study the eigenvalues of regular elements in G. Actually, for most of this chapter, we focus on the particular cases of Euclidean reflection groups, even Weyl groups.

As already stated, we assume that V is a finite dimensional vector space over a *field* $\mathbb{F}$ *of characteristic zero* and that $G \subset \mathrm{GL}(V)$ *is a finite pseudo-reflection group*. Let ξ be a primitive d-th root of unity belonging to $\mathbb{F}$, and let $\varphi \in G$ be an element of order d. As observed in (I-4), every eigenvalue is of the form ξ^k for some $1 \leq k < d$. In the case of regular elements, these exponents can be explicitly determined in terms of the "exponents" $\{m_1, \ldots, m_n\}$ of the pseudo-reflection group. Both exponents and degrees $\{d_1, \ldots, d_n\}$ of pseudo-reflection groups were introduced in §18-1. They are related by the rule $d_i = m_i + 1$ provided we consider them in the order $d_1 \leq \cdots \leq d_\ell$ and $m_1 \leq \cdots \leq m_\ell$.

***Theorem A* (Springer)** *Let $\varphi \in G$ be a regular element of order d with a primitive d-th root of unity $\xi \in F$ as a regular eigenvalue. If $\{m_1, \ldots, m_n\}$ are the exponents of G. Then the eigenvalues of φ are $\{\xi^{-m_1}, \ldots, \xi^{-m_n}\}$.*

In the case of Coxeter elements, we can obtain even stronger, and more detailed, results than in Theorem A. Let $W \subset O(\mathbb{E})$ be an irreducible finite Euclidean reflection group. Let

$$N = \text{the number of reflecting hyperplanes of } W.$$

Recall from §29-4 that the Coxeter number

$$h = 2N/\ell$$

gives the order of Coxeter elements in W. (Recall, from Remark 2 in §32-1, that the study of regular elements in Euclidean reflection groups involves complexification.) In particular, as observed in §32-1, Coxeter elements are regular with a primitive h-th root of unity as a regular eigenvalue.

***Theorem B* (Coxeter)** *Let $W \subset O(\mathbb{E})$ be an irreducible Euclidean reflection group with exponents $\{m_1, \ldots, m_\ell\}$. Let ω be a Coxeter element of W with the primitive*

h-th root of unity ξ as a regular eigenvalue for ω (over $\mathbb{C}$) then ω has eigenvalues $\{\xi^{m_1}, \ldots, \xi^{m_\ell}\}$ (over $\mathbb{C}$).

Observe that, if we assume $m_1 \leq \cdots \leq m_\ell$, then Theorem B implies $m_1 = 1$. We already have an independent proof of this fact (see §18-6). However, there are also other relations between the exponents that can be deduced from the above theorem. In particular, we have a duality relation.

Corollary A *Let $W \subset O(\mathbb{E})$ be an irreducible Euclidean reflection group with exponents $m_1 \leq \cdots \leq m_\ell$. Then*

$$m_i + m_{\ell-i+1} = h \quad \textit{for each } i.$$

Since $m_1 = 1$, this leads to a new characterization of the Coxeter number in terms of invariant theory.

Corollary B $h = m_\ell + 1 = d_\ell$.

The first equality comes from Corollary A, whereas the second is true by definition. If we restrict to Weyl groups, then Theorem B can be used to deduce an impressive result about exponents.

Corollary C *Let $W \subset O(\mathbb{E})$ be an irreducible Weyl group. If $1 \leq m < h$ and $(m, h) = 1$, then m is an exponent of G. In particular, rank $W \geq \phi(h)$ where $\phi =$ the Euler function.*

The following provides an concrete example of these corollaries. In particular, it provides a striking illustration of the power of Corollary C.

Example: Weyl group $W = W(E_8)$ The Weyl group $W = W(E_8)$ has exponents $\{1, 7, 11, 13, 17, 19, 23, 29\}$. Observe that, by Corollary B, $h = 30$. Alternatively, we can also determine that $h = 30$ directly from the root system of E_8 as given in §8-7 by using the formula $h = 2N/\ell$. Moreover, by Corollary C, $h = 30$ then forces textitall the above exponents of $W(E_8)$. In addition, Corollary A is illustrated by the identities

$$h = 1 + 29 = 7 + 23 = 11 + 19 = 13 + 17.$$

Coxeter elements can actually be characterized in terms of their eigenvalue properties. It can be shown:

Theorem C *Let $W \subset O(\mathbb{E})$ be an irreducible Euclidean reflection group with Coxeter number h. Then $\varphi \in W$ is a Coxeter element if and only if φ has an h-th root of unity as an eigenvalue (over $\mathbb{C}$).*

We have already justified Corollary B, provided the other results of this section can be proved. In §32-3, we shall look at eigenvalues of regular elements in pseudo-reflection groups and prove Theorem A. In §32-4, we shall look at eigenvalues of regular elements of Euclidean reflection group and prove Theorems B and C, as well as Corollaries A and C.

Remark: We end this section by remarking upon another consequence of Theorem B. Let $W \subset O(\mathbb{E})$ be an irreducible finite Euclidean reflection group with Coxeter number h and let ω be a Coxeter element of W. Proposition 18-6 entails that, for an irreducible finite Euclidean reflection group $W \subset O(\mathbb{E})$, not only is $m_1 = 1$, but also $2 \leq m_i < h$ for $i = 2, 3, \ldots, \ell$. So if ξ is a primitive h-th root of unity that is a regular eigenvalue of ω, then Theorem B implies

$$(*) \qquad \dim V(\omega, \xi) = 1.$$

This fact was required in the proof of Theorem 28-6, but was left unverified at that time. So the proof of Theorem 28-6 has now been completed and it is legitimate to assume that the centralizer of a Coxeter element ω consists of the powers of ω. This structure theorem for centralizers is needed in this chapter. It will be used in §32-4 for the proof of Theorem C.

32-3 The proof of Theorem 32-1A

This section establishes the connection between invariant theory and the eigenvalues of a regular element, as described in Theorem 32-1A. We assume that V is a finite dimensional vector space over a *field* $\mathbb{F}$ *of characteristic zero* and that $G \subset \mathrm{GL}(V)$ *is a finite pseudo-reflection group.* As usual, let $\{d_1, \ldots, d_n\}$ and $\{m_1, \ldots, m_n\}$ denote the degrees and exponents of the group $G \subset \mathrm{GL}(V)$. Let φ be a regular element of order d. As in Property (I-3) of §32-1, pick a regular vector x and a primitive d-th root of unity ξ such that

$$\varphi \cdot x = \xi x.$$

As observed in Property (I-4), φ is diagonalizable and every eigenvalue is of the form ξ^k for some $1 \leq k < d$. Expand $t_1 = x$ to a basis $\{t_1, \ldots, t_n\}$ of V consisting of eigenvectors of φ. Let $\{\xi^{k_1}, \ldots, \xi^{k_n}\}$ be the eigenvalues of φ corresponding to $\{t_1, \ldots, t_n\}$, i.e.,

$$\varphi \cdot t_i = \xi^{k_i} t_i.$$

We think of the elements of $S^* = S(V^*)$ as polynomial functions on V. Let $\{\alpha_1, \ldots, \alpha_n\}$ be the dual basis in V^* of the basis $\{t_1, \ldots, t_n\}$ of V. The Kronecker pairing

$$\alpha_i(t_j) = \delta_{ij}$$

plus the relation

$$\varphi^{-1} \cdot \alpha_i(t_j) = \alpha_i(\varphi \cdot t_j)$$

then forces

$$\varphi \cdot \alpha_i = \xi^{-k_i} \alpha_i.$$

We can write

$$S^* = \mathbb{F}[\alpha_1, \ldots, \alpha_n] \quad \deg \alpha_i = 1$$

$$R^* = S^{*G} = \mathbb{F}[\omega_1, \ldots, \omega_n] \quad \deg \omega_i = d_i,$$

where each ω_i is a polynomial in $\{\alpha_1, \ldots, \alpha_n\}$. (The identity $\deg \omega_i = d_i$ follows from the Remark at the end of §17-2.) We can deduce some facts about these polynomials. If $J^* = \det[\frac{\partial \omega_i}{\partial \alpha_j}]_{n\times n}$ is the Jacobian as defined in §21-1, then

$$J^*(t_1) \neq 0.$$

For, by §21-3, $J^* = \lambda \Omega^*$, where $\lambda \neq 0$ and $\Omega^* = \prod \alpha_s$. Moreover, t_1 regular implies $\alpha_s(t_1) \neq 0$ for each s. So $\Omega^*(t_1) \neq 0$ and, thus, $J^*(t_1) \neq 0$ as well.

So there is a permutation σ of $\{1, \ldots, n\}$ such that

$$\frac{\partial \omega_i}{\partial \alpha_{\sigma(i)}}(t_1) \neq 0 \quad \text{for } 1 \leq i \leq n.$$

Consequently, when we use the standard basis $\{\alpha^E = \alpha_1^{e_1} \cdots \alpha_n^{e_n}\}$ of $S^* = \mathbb{F}[\alpha_1, \ldots, \alpha_n]$ we have, up to a nonzero constant,

$$\frac{\partial \omega_i}{\partial \alpha_{\sigma(i)}} = \alpha_1^{d_i - 1} + \text{other terms.}$$

Hence

$$\omega_i = \alpha_1^{d_i-1}\alpha_{\sigma(i)} + \text{other terms.}$$

If we apply φ, we have

$$\varphi \cdot \omega_i = [\xi^{-(d_i-1)}\alpha_1^{d_i-1}][\xi^{-k_{\sigma(i)}}\alpha_{\sigma(i)}] + \text{other terms.}$$

The identity $\varphi \cdot \omega_i = \omega_i$ then forces

$$\xi^{-(d_i-1)}\xi^{-k_{\sigma(i)}} = 1.$$

So

$$\xi^{k_{\sigma(i)}} = \xi^{-(d_i-1)} = \xi^{-m_i}.$$

32-4 Eigenvalues in Euclidean reflection groups

In this section, we prove the results of §32-2. We shall prove the results about eigenvalues of Coxeter elements as stated in Theorems B and C, as well as the relations for exponents as given in Corollaries A and C. In all that follows, let $W \subset O(\mathbb{E})$ be *an irreducible Euclidean reflection group* with exponents $m_1 \leq \cdots \leq m_\ell$. Let ω be a Coxeter element of W. As in §32-2, ω has order $h = 2N/\ell$. We shall pass to the complex numbers and assume that W is acting on $V_{\mathbb{C}} = \mathbb{C}^\ell$.

Proof of Theorem 32-2B We know that ω is a regular element. So, by Theorem A, we can pick an h-th primitive root of unity ξ such that ω has eigenvalues $\{\xi^{-m_1}, \ldots, \xi^{-m_\ell}\}$. Since ω is a real transformation, its complex eigenvalues must occur in conjugate pairs. It follows that the eigenvalues $\{\xi^{-m_i}, \ldots, \xi^{-m_\ell}\}$ can be arranged so that, for each i,

$$m_i + m_{\ell-i+1} \equiv 0 \pmod{h}.$$

Since $\xi^{-m_i} = \xi^{m_{\ell-i+1}}$, it follows that $\{\xi^{m_1}, \ldots, \xi^{m_\ell}\}$ is a rearrangement of $\{\xi^{-m_1}, \ldots, \xi^{-m_\ell}\}$ and Theorem B is proved.

Proof of Corollary 32-2A In view of the identity $m_i + m_{\ell-i+1} \equiv 0 \pmod h$ established above, it suffices to show that

$$(*) \qquad m_i < h \quad \text{for all } i$$

because $m_i + m_j \equiv 0 \pmod h$, along with $0 < m_i + m_j < 2h$, then forces $m_i + m_j = h$. Recall that

(i) $N = \frac{1}{2}h\ell$;
(ii) $m_1 + \cdots + m_\ell = N$.

For (i), see §29-4. For (ii), see §18-1. Write

$$m_i = q_i h + r_i, \quad \text{where } 0 \leq r_i < h.$$

We want to show $m_i = r_i$. By Theorem B, $\{\xi^{r_i}, \ldots, \xi^{r_\ell}\}$ are the eigenvalues of ω. Since ω is a real transformation, its complex eigenvalues occur in conjugate pairs. So $\{h - r_1, \ldots, h - r_\ell\}$ is a rearrangement of $\{r_1, \ldots, r_\ell\}$. The equality

$$h - r_1 + \cdots + h - r_\ell = r_1 + \cdots + r_\ell$$

forces

(iii) $r_1 + \cdots + r_\ell = \frac{1}{2}h\ell = N$.

A comparison of (ii) and (iii) yields $r_i = m_i$ for all i. We now have $(*)$ and, hence, Corollary A.

Proof of Corollary 32-2C Let $W \subset GL_\ell(\mathbb{Z})$ be a Weyl group. The distinguishing property of Weyl groups needed to prove Corollary C is:

Lemma *Let $\varphi \in W$ be an element of order d. Each primitive d-th root of unity occurs as an eigenvalue of φ with the same multiplicity.*

It follows from this lemma that a regular element of order d has every primitive d-th root of unity as an eigenvalue. Let h be the Coxeter number of W. As in Theorem B, let ξ be a primitive h-th root of unity which is a regular eigenvector for the Coxeter element $\omega \in W$. If $(m, h) = 1$, then ξ^m is also a primitive h-th root of unity. Hence it is an eigenvalue of ω. It follows from Theorem B, and the fact that $1 \leq m < h$, that m must agree with one of the exponents $\{m_1, \ldots, m_\ell\}$. So we are left with proving the lemma.

Proof of Lemma We need to recall some facts from linear algebra. Let $p(T) \in \mathbb{Z}[T]$ be the characteristic polynomial of ϕ.

(a) When we pass to $\mathbb{C}[T]$, then $p(T)$ splits into linear factors

$$p(T) = (T - \lambda_1)^{m_1} \cdots (T - \lambda_k)^{m_k},$$

where $\{\lambda_1, \ldots, \lambda_k\}$ are the eigenvalues of ϕ and m_i is the multiplicity of λ_i as an eigenvalue of ϕ, i.e.,

$$(*) \qquad m_i = \dim V(\phi, \lambda_i).$$

We observe that each λ_i, being an eigenvalue of ϕ, is a d-th root of unity.

(b) Next we work in $\mathbb{Z}[T]$. The *cyclotomic polynomials* $\Phi_k(T) \in \mathbb{Z}[T]$ are defined by the recursive formula

$$T^n - 1 = \prod_{k|n} \Phi_k(T).$$

They are irreducible in $\mathbb{Z}[T]$ but decompose over $\mathbb{C}$ as a product

$$(**) \qquad \Phi_k(T) = \prod (T - \zeta),$$

where $\{\zeta\}$ are the primitive k-th roots of unity. In particular, Φ_k is the irreducible polynomial over $\mathbb{Z}$ for the primitive k-th root of unity.

Since every root of $p(T)$ is an d-th root of unity, it follows that $p(T) \in \mathbb{Z}[T]$ is a product of cyclotomic polynomials. When we pass to $\mathbb{C}$, it follows from $(**)$ that the multiplicity of each primitive d-th root of unity, as a root of $p(T)$, is the same and is obtained by counting the number of copies of the d-th cyclotomic polynomial in the cyclotomic decomposition of $p(T)$. The lemma now follows from $(*)$. ■

Proof of Theorem 32-2C Let $W \subset O(\mathbb{E})$ be *an irreducible Euclidean reflection group* with degrees $d_1 \leq \cdots \leq d_\ell$. Let h be the Coxeter number of W. Since Corollary 32-2B is now known to hold, we have

$$(*) \qquad h = d_\ell.$$

We also know from Proposition 18-6 that $d_1 = 2$ while $d_i \geq 3$ for $i = 2, 3, \ldots, \ell$. The relation $m_i + m_{\ell-i+1} = h$ of Corollary 32-2A then forces

$$(**) \qquad h > d_1, d_2, \ldots, d_{\ell-1}.$$

Pick a Coxeter element $\omega \in W$. The order of ω is h. In view of Remark (I-4) of §32-1, we can choose an h-th primitive root of unity ξ that is a regular eigenvalue for ω. Since all Coxeter elements of W are conjugate (see §29-2), it follows that ξ is an eigenvalue for every Coxeter element of W. Let

$$\mathcal{C} = \text{the conjugacy class of Coxeter element}$$

$$\mathcal{D} = \text{the elements of W having } \xi \text{ as an eigenvalue.}$$

By the above, we have an inclusion

$$\mathcal{C} \subset \mathcal{D}.$$

We shall prove that $\mathcal{C} = \mathcal{D}$ by a counting argument. Namely, we can show that

$$|\mathcal{C}| = d_1 d_2 \cdots d_{\ell-1} = |\mathcal{D}|.$$

(i) $|\mathcal{C}| = d_1 d_2 \cdots d_{\ell-1}$.

Since every Coxeter element is conjugate to a fixed one (say ω), it follows that

$$|\mathcal{C}| = |W/Z(\omega)| = |W|/|Z(\omega)|.$$

It was remarked at the end of §32-2 that Theorem 32-2B provided the final step needed to complete the proof of Theorem 28-6. So the proof of Theorem 28-6 is now complete and we have $Z(\omega) = \{\omega^i\}$. It follows from identity $(*)$ above that

$$|Z(\omega)| = d_\ell.$$

In view of the identity $|W| = d_1 \cdots d_\ell$ from §18-1, we have identity (i).

(ii) $|\mathcal{D}| = d_1 d_2 \cdots d_{\ell-1}$.

The Pianzola-Weiss polynomial for the h-th primitive root of unity ξ was defined in Theorem 31-1B. Identities $(*)$ and $(**)$ say that the Pianzola-Weiss polynomial for ξ is

$$P = d_1 d_2 \cdots d_{\ell-1}(T + m_\ell).$$

The coefficient of T counts the number of elements of W having ξ as an eigenvalue. Consequently, the number of elements with ξ as an eigenvalue is $d_1 d_2 \cdots d_{\ell-1}$.

33 Ring of invariants and eigenvalues

The results in this chapter are due to Springer [1]. The main concern of this chapter is, once again, the study of the eigenspaces of elements in pseudo-reflection groups. This section can be regarded as the beginning of the study of conjugacy classes in pseudo-reflection groups (as opposed to just the case of Euclidean reflection groups). We shall be studying the relation between different eigenspaces and, in particular, the question of when eigenspaces are related through the action of G. As we shall see, the arguments of this chapter fit into the framework of algebraic geometry. The key point is that rings of invariants have a natural interpretation, in the context of algebraic geometry, as the coordinate ring of orbit spaces.

33-1 Main results

Let V be a finite dimensional vector space over the field $\mathbb{F}$ and let $G \subset \mathrm{GL}(V)$ be a finite group. The eigenspaces $V(\varphi, \xi)$ for elements of G were introduced and studied in Chapter 31. In this chapter, we demonstrate that these eigenspaces can be further analyzed in the context of algebraic geometry. We shall be studying the role of eigenspaces of maximal dimension and how they are related to each other by the action of G on V. As usual, we shall let

$$S = S(V) \quad \text{and} \quad S^* = S(V^*)$$
$$R = S^G \quad \text{and} \quad R^* = S^{*G}.$$

We can regard S^*, and hence R^*, as polynomial functions on V. The following is the basic relation between the polynomial functions R^* and the action of G on V.

Theorem A *Given $x, y \in V$, then $y = \varphi \cdot x$ for some $\varphi \in G$ if and only if $\gamma(x) = \gamma(y)$ for all $\gamma \in R^*$.*

By using Theorem A, we can deduce a number of results about eigenvalues of elements of G. In all that follows, *let $d \geq 2$ be a fixed integer and let ξ be a fixed primitive d-th root of unity.* The following result is an easy consequence of Theorem A.

Theorem B *Suppose that $\xi \in \mathbb{F}$. Given $x \in V$, then $\varphi \cdot x = \xi x$ for some $\varphi \in G$ if and only if $\gamma(x) = 0$ for all $\gamma \in R^*$ of degree $\not\equiv 0$ (mod d).*

By introducing some machinery from algebraic geometry, we can force a number of further results about eigenspaces. For each $\varphi \in G$ and $\xi \in \mathbb{F}$, let $V(\varphi, \xi)$, denote the eigenvalue space

$$V(\varphi, \xi) = \{x \in V \mid \varphi \cdot x = \xi x\}.$$

These subspaces were studied in Chapter 31 and restrictions were obtained there about their possible dimensions. Let $G \subset \mathrm{GL}(V)$ be *a finite nonmodular pseudo-reflection group.* Let $\{d_1, \dots, d_\ell\}$ be the degrees of G. Let

$$\alpha(d) = \#\{d_i \mid d \text{ divides } d_i\}.$$

It follows from Theorem 31-1B that, for a primitive d-th root of unity ξ, we have

$$\max_{\varphi\in G} \dim V(\varphi,\xi) = \alpha(d)$$

(i.e., the polynomial $P_d(T)$ determined by that theorem has degree $\alpha(d)$). We shall now also show:

Theorem C *Let $G \subset \mathrm{GL}(V)$ be a finite nonmodular pseudo-reflection group. If $\xi \in \mathbb{F}$, then every $V(\phi,\xi)$ is contained in some $V(\varphi,\xi)$ of dimension $\alpha(d)$.*

The collection $\{V(\varphi,\xi)\}$ is permuted by G. The action is determined by the rule

$$\tau \cdot V(\varphi,\xi) = V(\tau\varphi\tau^{-1},\xi).$$

Our next theorem asserts that G acts transitively on the eigenspaces of maximal dimension.

Theorem D *Let $G \subset \mathrm{GL}(V)$ be a finite nonmodular pseudo-reflection group. Suppose $\xi \in \mathbb{F}$. If $\dim V(\varphi_1,\xi) = \dim V(\varphi_2,\xi) = \alpha(d)$, then there exists $\tau \in G$ such that $\tau \cdot V(\varphi_1,\xi) = V(\varphi_2,\xi)$.*

The above result is, in a sense, incomplete. We would like to know not only when $\tau \cdot V(\varphi_1,\xi) = V(\varphi_2,\xi)$, i.e., when

$$V(\tau\varphi_1\tau^{-1},\xi) = V(\varphi_2,\xi),$$

but also when

$$\tau\varphi_1\tau^{-1} = \varphi_2.$$

In other words, we would like to know about the conjugacy relation between elements of G. Unfortunately, the above data concerning eigenspaces only provides partial information on this topic because $\tau\cdot V(\varphi_1,\xi) = V(\varphi_2,\xi)$ only tells us that $\tau\varphi_1\tau^{-1}$ and φ_2 agree on the subspace $\tau \cdot V(\varphi_1,\xi) = V(\varphi_2,\xi)$. However, there is one case when a stronger result can be obtained. It will be shown in Chapter 34 that, in the case of Weyl groups, regular elements of a fixed order d form a single conjugacy class. So we can view the present chapter as the beginning of the study of conjugacy classes in pseudo-reflection groups.

Theorems A and B will be proved in §33-3. The other results concerning the eigenspaces $V(\varphi,\xi)$ will be proved in §33-4. Before proving these results, however, we want to first briefly discuss in §33-2 some basic facts about algebraic geometry. For the above results are motivated by, and fit into, the framework of algebraic geometry.

33-2 Algebraic geometry

This section introduces some fundamental concepts from algebraic geometry. References for the elementary notions from algebraic geometry used in this chapter are Hartshorne [1] or Kendig [1].

We shall assume that $\mathbb{F}$ is algebraically closed. This is a traditional hypothesis for algebraic geometry. An *affine variety* $X \subset \mathbb{F}^n$ is the set of zeros of a collection of polynomials. More precisely, if $V = \mathbb{F}^n$, then the collection of polynomials generates an ideal $I \subset S^*$ and the variety $X = X(I)$ is defined by the rule

$$X = \{x \in V \mid \gamma(x) = 0 \text{ for all } \gamma \in I\}.$$

So an algebraic variety is the set of zeros of an ideal $I \subset S^*$ and is denoted accordingly. An affine variety X is *irreducible* if $X = X_1 \cup X_2$, where X_1 and X_2 are varieties implies that $X = X_1$ or $X = X_2$. The variety $X = X(I)$ is irreducible if and only if the ideal I is prime. Notably, the linear subspaces of V are determined by linear equations and, so, are irreducible affine varieties. Every affine variety can be broken up, uniquely, into irreducible components. As an example, the variety $X \subset \mathbb{F}^2$ given by

$$X = \{(x, y) \mid xy = 0\}$$

decomposes into the two irreducible linear subspaces $X = X_1 \cup X_2$, where

$$X_1 = \{(x, y) \mid x = 0\} \quad \text{and} \quad X_2 = \{(x, y) \mid y = 0\}.$$

The *coordinate ring* of $X = X(I)$ is defined to be the quotient ring S^*/I. In particular, V itself is the affine algebraic variety with coordinate ring S^*. The *dimension* of a variety is the maximal number of algebraically independent functions in its coordinate ring. In the case of a linear subspace of V, its dimension, as a vector space, agrees with its dimension as a variety.

Lastly, a variety has a canonical topology, called the *Zariski topology*, which is defined on X by letting the subvarieties of X be its closed sets. The open sets of X have the property that each is dense in X. The intersection of any two nontrivial open sets is again nontrivial. So this is a very weak topology.

Remark: Theorem 33-1A asserts that the ring of invariants $R^* = S^{*G}$ is the coordinate ring of a suitable variety. Namely, we can give the orbit space V/G an affine algebraic variety structure such that R^* is the coordinate ring of V/G. We shall not be explicitly using this fact. However, the approach of this chapter is certainly motivated by it. In this chapter, we are basically using R^* to analyze G orbits in V.

33-3 The ring of invariants as a coordinate ring

In this section, we prove Theorems A and B of §33-1. We continue to use the notation, and conventions, of §33-1. In particular, we continue to *regard S^*, and hence R^*, as polynomial functions on V.* We also remark upon another fact. The action of G on S^* and on V are related by the rule

$$\varphi \cdot \gamma(x) = \gamma(\varphi^{-1} \cdot x).$$

Before proving Theorems A and B, we first establish:

Proposition *Let p and q be prime ideals of S^*. If $p \cap R^* = q \cap R^*$, then $p \subset \varphi \cdot q$ for some $\varphi \in G$.*

The proposition will follow from the next two lemmas.

Lemma A *Let p and q be prime ideals of S^*. If $p \cap R^* = q \cap R^*$, then*

$$p \subset \bigcup_{\varphi \in G} \varphi \cdot q.$$

Proof Pick $x \in p$. Then

$$\left[\prod_{\varphi \in G} \varphi \cdot x\right] \in p \cap R^* = q \cap R^* \subset q.$$

Since q is a prime ideal, it follows that $\varphi \cdot x \in q$ for some $\varphi \in G$. Hence $x \in \varphi^{-1} \cdot q$. ∎

Lemma B *Let $q_1, \ldots, q_n$ be prime ideals of S^*. Given an ideal $a \subset S^*$, where $a \subset \bigcup_{i=1}^n q_i$, then $a \subset q_i$ for some i.*

Proof We shall prove the contrapositive version of this lemma. Namely, we shall prove that

$$a \not\subset q_i \quad \text{for all } i \text{ implies that } a \not\subset \bigcup_{\varphi \in G} q_i.$$

We proceed by induction on n. The initial case $n = 1$ is trivial. Consider the general case n. The $n - 1$ case tells us that

$$a \not\subset \bigcup_{i \neq k} q_i \quad \text{for each } 1 \leq k \leq n.$$

Hence, for each $1 \leq k \leq n$, we can find $x_k \in a$ such that

$$(*) \qquad x_k \notin q_i \quad \text{for } i \neq k.$$

If, for any k, $x_k \notin q_k$, then $x_k \notin \bigcap_{i=1}^n q_i$, and we are done. So suppose as well that

$$(**) \qquad x_k \in q_k \quad \text{for all } k.$$

Let

$$y = \sum_{i=1}^{n} x_1 x_2 \cdots \hat{x}_i \cdots x_n.$$

We have $y \in a$. On the other hand, $y \notin q_i$ for any i because assumption $(**)$ tells us that all the summands of y except $x_1 x_2 \cdots \hat{x}_i \cdots x_n$ belong to q_i. Thus $y \in q_i$ forces $x_1 x_2 \cdots \hat{x}_i \cdots x_n \in q_i$. Since q_i is prime, this forces $x_k \in q_i$ for some $i \neq k$, which contradicts $(*)$. ∎

Combining Lemma A and Lemma B, we have the above proposition. We now turn to the proofs of Theorems A and B.

Proof of Theorem 33-1A First of all, assume $y = \varphi \cdot x$. Then, for any $\gamma \in R^*$,

$$\gamma(y) = \gamma(\varphi \cdot x) = \varphi^{-1} \cdot \gamma(x) = \gamma(x).$$

Conversely, assume $\gamma(x) = \gamma(y)$ for all $\gamma \in R^*$. For each $a \in V$, we can define the evaluation map

$$e_a : S^* \to \mathbb{F}$$
$$\gamma \mapsto \gamma(a).$$

Then $\ker e_a$ is a maximal ideal of S^*. It is generated by the hyperplane $H_a \subset V^*$, where

$$H_a = \{\gamma \in V^* \mid \gamma(a) = 0\}.$$

For any $\varphi \in G$, $\varphi \cdot a = b$ if and only if $\varphi \cdot H_a = H_b$. Thus $\varphi \cdot a = b$ if and only if $\varphi \cdot (\operatorname{Ker} e_a) = \operatorname{Ker} e_b$. So $\operatorname{Ker} e_a$ determines $a \in V$ uniquely.

Our assumption about x and y can be formulated as $R^* \cap \operatorname{Ker} e_x = R^* \cap \operatorname{Ker} e_y$. It follows from the previous proposition that $\operatorname{Ker} e_y \subset \varphi \cdot (\operatorname{Ker} e_x) = \operatorname{Ker} e_{\varphi \cdot x}$ for some $\varphi \in G$. Since the ideals are maximal, we have $\operatorname{Ker} e_y = \operatorname{Ker} e_{\varphi \cdot x}$. Consequently, $y = \varphi \cdot x$.

Proof of Theorem 33-1B First of all, suppose $\varphi \cdot x = \xi x$. Given $\alpha \in R^*$ of degree k, then

$$\gamma(x) = \varphi^{-1}\gamma(x) = \gamma(\varphi \cdot x) = \gamma(\xi x) = \xi^k \gamma(x).$$

If $k \not\equiv 0 \pmod{d}$, then $\xi^k \neq 1$ and $\gamma(x) = 0$.

Conversely, suppose $\gamma(x) = 0$ for all $\gamma \in R^*$ of degree $\not\equiv 0 \pmod{d}$. The equation $\gamma(\xi x) = \xi^k \gamma(x)$ for γ of degree k then tells us that $\gamma(\xi x) = \gamma(x)$ for all $\gamma \in R^*$. By Theorem A, $\xi x = \varphi \cdot x$ for some $\varphi \in G$. ■

33-4 Eigenspaces

In this section, we are concerned with Theorems C and D of §33-1. We continue to use the notation and conventions of §33-1. In particular, $d \geq 2$ will be a fixed integer and ξ will be a fixed primitive d-th root of unity. Since $G \subset \mathrm{GL}(V)$ is a finite nonmodular pseudo-reflection group, we can write

$$R^* = \mathbb{F}[\omega_1, \ldots, \omega_n]$$

(see §18-1). Let $d_i = \deg \omega_i$. Then Theorem 33-1B can be reformulated as stating that $\varphi \cdot x = \xi x$ for some $\varphi \in G$ if and only if $\omega_i(x) = 0$ whenever $d_i \not\equiv 0 \pmod{d}$. For each i, let $H_i \subset V$ be the hypersurface

$$H_i = \{x \in V \mid \omega_i(x) = 0\}$$

and let

$$H(d) = \bigcap_{d_i \not\equiv 0 \ (\mathrm{mod}\ d)} H_i.$$

Then Theorem B can be further restated as asserting that $H(d)$ gives all the eigenvectors associated with the eigenvector ξ for any $\varphi \in G$. In other words, if, for each $\varphi \in G$, we let

$$V(\varphi, \xi) = \{x \in V \mid \varphi \cdot x = \xi x\},$$

then Theorem B is equivalent to the following.

Proposition *Suppose that $\xi \in \mathbb{F}$. Then $H(d) = \bigcup_{\varphi \in G} V(\varphi, \xi)$.*

In particular, this proposition gives a decomposition of the algebraic variety $H(d)$ into irreducible components. We now set about proving Theorems C and D.

Proof of Theorem 33-1C First of all,

$$\bigcap_{i=1}^{n} H_i = 0.$$

For, if $x \in \bigcap_{i=1}^{n} H_i$, then $\omega_i(x) = 0$ for each i and, so, $\gamma(x) = 0$ for all $\gamma \in R^*$. By Theorem 33-1A, $x = \varphi \cdot 0$ for some $\varphi \in G$. So $x = 0$.

It follows that the hypersurfaces $\{H_1, \ldots, H_n\}$ *intersect properly*, i.e., given irreducible components $C_k \subset H_k$, then $C_{i_1} \cap \cdots \cap C_{i_r}$ has dimension $n - r$ for any $\{i_1, \ldots, i_r\}$. In particular, the dimension of

$$H(d) = \bigcap_{d_i \not\equiv 0 \ (\mathrm{mod}\ d)} H_i$$

at every point is $\alpha(d)$. Using the above proposition, write

$$H(d) = \bigcup_{\varphi \in G} V(\varphi, \xi).$$

Suppose that $V(\varphi, \xi)$ is maximal (i.e., not contained in any $V(\phi, \xi)$ of higher dimension). As observed in §32-2, it is an irreducible component of $H(d)$. Consequently,

$$\dim V(\varphi, \xi) = \alpha(d).$$

Proof of Theorem 33-1D Suppose that $\dim V(\varphi_1, \xi) = \dim V(\varphi_2, \xi) = \alpha(d)$. We want to show that there exists $\tau \in G$ such that

$$\tau \cdot V(\varphi_1, \xi) = V(\varphi_2, \xi).$$

Arrange the $\{\omega_i\}$ so that

$$\{\omega_1, \ldots, \omega_\alpha\} \text{ have degrees} = 0 \ (\mathrm{mod}\ d),$$

while

$$\{\omega_{\alpha+1}, \ldots, \omega_n\} \text{ have degrees} \neq 0 \ (\mathrm{mod}\ d).$$

Before proving the theorem, we first prove:

Lemma *If $\dim V(\varphi, \xi) = \alpha(d)$ then $\{\omega_1, \ldots, \omega_\alpha\}$ restricted to $V(\varphi, \xi)$ are algebraically independent.*

Proof By the definition of $H(d)$, $\omega_{\alpha+1} = \cdots = \omega_n = 0$ on $H(d)$ and, hence, on $V(\varphi, \xi)$. So the map of algebraic varieties

$$F\colon V(\varphi, \xi) \to \mathbb{F}^{\alpha}$$
$$F(x) = \big(\omega_1(x), \ldots, \omega_\alpha(x)\big)$$

has fibre $F^{-1}(0) = \bigcap_{i=1}^{n} H_i = \{0\}$. On the other hand, given a morphism

$$G\colon U \to W$$

of algebraic varieties then, for any $x \in G(U) \subset W$,

$$\dim G^{-1}(x) \geq \dim U - \dim G(U).$$

In the case of F, we have $0 \geq \alpha - \dim F\big(V(\varphi, \xi)\big)$. So $\dim F\big(V(\varphi, \xi)\big) \geq \alpha$. ■

We now turn to the proof of Theorem D. Suppose

$$\dim V(\varphi_1, \xi) = \dim V(\varphi_2, \xi) = \alpha(d).$$

Let

$$U_1 = V(\varphi_1, \xi) - \Big[\bigcup_{\phi \neq \varphi_1} V(\phi, \xi)\Big]$$
$$U_2 = V(\varphi_2, \xi) - \Big[\bigcup_{\phi \neq \varphi_2} V(\phi, \xi)\Big].$$

Then $U_1 \subset V(\varphi_1, \xi)$ and $U_2 \subset V(\varphi_2, \xi)$ are Zariski open (dense) sets. Let

$$F_1\colon V(\varphi_1, \xi) \to \mathbb{F}^{\alpha}$$
$$F_2\colon V(\varphi_2, \xi) \to \mathbb{F}^{\alpha}$$

be defined, as in the proof of the above lemma, by the tuple $(\omega_1, \ldots, \omega_\alpha)$. These are open maps (i.e., open sets are mapped to open sets). So the lemma shows that $F_1(U_1)$ and $F_2(U_2)$ are nonempty Zariski open subsets of the affine space $\mathbb{F}^{\alpha}$. Thus they have a nontrivial intersection and we can find

$$x \in U_1 \subset V(\varphi_1, \xi) \quad \text{and} \quad y \in U_2 \subset V(\varphi_2, \xi)$$

such that

$$F_1(x) = F_2(y).$$

By the definition of $H(d)$,

$$\omega_{\alpha+1} = \cdots = \omega_n = 0 \quad \text{on } V(\varphi_1, \xi) \text{ and on } V(\varphi_2, \xi).$$

It follows that

$$\omega_i(x) = \omega_i(y) \quad \text{for } 1 \leq i \leq n.$$

By Theorem 33-1A, $y = \tau \cdot x$ for some $\tau \in G$. So

$$y \in \tau \cdot V(\varphi_1, \xi) = V(\tau\varphi_1\tau^{-1}, \xi).$$

However, recall that $y \in U_2 \subset V(\varphi_2, \xi)$. So

$$y \notin V(\phi, \xi) \quad \text{if } \phi \neq \varphi_2.$$

Comparing these two facts, we conclude that $\tau \cdot V(\varphi_1, \xi) = V(\varphi_2, \xi)$.

34 Properties of regular elements

In this chapter we continue to use invariant theory and algebraic geometry to analyze the regular elements of pseudo-reflection groups. We shall apply the machinery from Chapter 33 to study regular elements of pseudo-reflection groups. It has been demonstrated in §29-5 that, in the case of Euclidean reflection groups, Coxeter elements are regular. The properties studied in this section have already been established for Coxeter elements. We shall be asking in this chapter to what extent certain properties generalize from Coxeter elements to regular elements in arbitrary pseudo-reflection groups. The results of this chapter are taken from Springer [2].

34-1 Properties of regular elements

Let V be a finite dimensional vector space over a field $\mathbb{F}$ of characteristic zero. Let $G \subset \mathrm{GL}(V)$ be a finite pseudo-reflection group. Regular elements of pseudo-reflection groups were defined and studied in Chapter 32. In this chapter, we use the machinery of Chapter 33 to continue our study of regular elements. Since regular elements can be viewed as generalizations of Coxeter elements, it might be hoped that some of the properties established in previous chapters for Coxeter elements would extend to all regular elements.

The very first property established for Coxeter elements was that they form a single conjugacy class in their Euclidean reflection group. Does this property extend to all regular elements? Is it possible that, for any pseudo-reflection group, the regular elements of a fixed order form a single conjugacy class? There is one case for which the answer is positive, namely for Weyl groups.

Theorem A **(Springer)** *Let W be a Weyl group. Then the regular elements of any fixed order d form a single conjugacy class.*

We can show that, given a finite pseudo-reflection group $G \subset \mathrm{GL}(V)$ and a regular element $\varphi \in G$ of order d, then every regular element of order d in G is conjugate to φ^k for some $k \geq 1$ where k is prime to d. So the content of Theorem A amounts to asserting that all the powers of a regular element lie in the same conjugacy class.

Unfortunately, this type of result only holds for Weyl groups. As the next example shows, Theorem A does not even extend to Euclidean reflection groups. Recall, from §1-3 and §1-4, that every dihedral group acts on the plane as an Euclidean reflection group but that only $D_2 = \mathbb{Z}/2\mathbb{Z}$, $D_3 = \Sigma_3$, $D_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $D_6 = W(G_2)$ are Weyl groups (see §9 and §10).

Example 1: Dihedral Group D_5 Consider the dihedral group D_5 acting on the Euclidean plane in the manner described in §1-5. This action realizes D_5 as a two-dimensional Euclidean reflection group. Let ω be a Coxeter element of D_5. Then ω is a rotation of order 5. Hence if we work over the complex numbers, there exists

a primitive fifth root of unity ξ such that

$$\omega = \begin{bmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{bmatrix} \quad \omega^2 = \begin{bmatrix} \xi^2 & 0 \\ 0 & \xi^{-2} \end{bmatrix}.$$

Both ω and ω^2 are regular and of order five. However, they have different eigenvalues ($\xi^2 \neq \xi$ or ξ^{-1}) and, so, cannot be conjugate.

We shall also prove another interesting general fact about centralizers of regular elements. We shall show that such centralizers act on certain eigenspaces as a pseudo-reflection group. Again, this generalizes a fact already proved (in Chapter 29) for Coxeter elements.

Given $\varphi \in G$ and $\xi \in \mathbb{F}$, consider the eigenvalue space

$$V(\varphi, \xi) = \{x \in V \mid \varphi \cdot x = \xi x\}.$$

The centralizer $Z(\varphi) \subset G$ of φ leaves $V(\varphi, \xi)$ invariant. For, given $\tau \in Z(\varphi)$ and $x \in V(\varphi, \xi)$, then

$$\varphi \cdot (\tau \cdot x) = (\varphi\tau) \cdot x = (\tau\varphi) \cdot x = \xi\tau \cdot x.$$

The following theorem deals with the action of $Z(\varphi)$ on $V(\varphi, \xi)$.

***Theorem B* (Springer)** *Suppose that $\mathbb{F}$ is algebraically closed. Let $\varphi \in G \subset \mathrm{GL}(V)$ be a regular element of order d with ξ, a primitive d-th root of unity, as a regular eigenvalue. Then*

(i) $Z(\varphi)$ acts on $V(\varphi, \xi)$ as a pseudo-reflection group;
(ii) The degrees of $Z(\varphi)$ are the degrees of G which are divisible by d.

If $\{d_1, \ldots, d_\ell\}$ are the degrees of G, then it follows from part (ii) of the theorem that:

Corollary *Let $\varphi \in G \subset \mathrm{GL}(V)$ be a regular element of order d. Then*

$$|Z(\varphi)| = \prod_{d_i \equiv 0 \pmod d} d_i.$$

Theorem B has been verified (implicitly) for Coxeter elements. We need only assemble a number of results from previous chapters. If $W \subset O(\mathbb{E})$ is an irreducible Euclidean reflection group with degrees $d_1 \leq \cdots \leq d_\ell$, then, by Corollary 32-2B, the Coxeter elements of W are of order d_ℓ. It was also demonstrated in §29-6 that the centralizer of the Coxeter element ω is the cyclic group $\{\omega^k\}$. In particular, we know that $|Z(\omega)| = d_\ell$. On the other hand, by the comments following Theorem 32-2B, we know that if ξ is a regular eigenvalue for ω then $\dim V(\omega, \xi) = 1$. The action of the group $\{\omega^k\}$ on $V(\omega, \xi)$ is that of a pseudo-reflection group.

We shall further illustrate Theorem B by applying it to two cases of Euclidean reflection groups, producing interesting reflection subgroups. Again, let $W \subset$

$O(\mathbb{E})$ be an irreducible Euclidean reflection group with degrees $d_1 \leq \cdots \leq d_\ell$, and let ω be a Coxeter element in W (of order d_ℓ). Since any power of a regular element is also regular, it follows that W has a regular element of order d for every divisor d of d_ℓ. If we *complexify* W (so as to guarantee the existence of the appropriate roots of unity) and apply Theorem B, then we can obtain subgroups of W that are complex pseudo-reflection groups. We shall give two examples, one rather simple and one fairly complicated.

Example 2: Dihedral Groups The dihedral group $W = D_m = \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, acting on the plane $V = \mathbb{R}^2$ as in §1-3, is a two-dimensional Euclidean reflection group with degrees $\{2, m\}$. The Coxeter element $\omega \in \mathbb{Z}/m\mathbb{Z}$ is a rotation of order m generating $\mathbb{Z}/m\mathbb{Z}$. If we work over the complex numbers, then we can write

$$\omega = \begin{bmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{bmatrix},$$

where ξ is a primitive m-th root of unity. The centralizer $Z(\omega) = \mathbb{Z}/m\mathbb{Z}$ acts on the one-dimensional eigenspace $V(\omega, \xi)$ as the most simple type of pseudo-reflection group. More generally, every power ω^k is regular and its centralizer is

$$Z(\omega^k) = D_m \quad \text{if order } \omega^k = 2$$

$$Z(\omega^k) = \mathbb{Z}/m\mathbb{Z} \quad \text{if order } \omega^k \neq 2.$$

Again, these centralizers act on $V(\omega, \xi)$, or on V as pseudo-reflection groups.

Example 3: Weyl Group $W = W(E_8)$ The reflection group $W = W(E_8)$ has degrees $\{2, 8, 12, 14, 18, 20, 24, 30\}$. So, by the discussion in Example 2, the Coxeter elements of W are of order 30 and the powers of Coxeter elements give regular elements of order 2, 3, 5, 6, 10, 15, and 30. By applying Theorem B, the centralizers of these elements have degrees as follows.

d	*degrees*
2	$2, 8, 12, 14, 18, 20, 24, 30$
3 or 6	$12, 18, 24, 30$
5 or 10	$20, 30$
15 or 30	30

Observe that most of these complex pseudo-reflection groups do not arise from Euclidean ones, because a Euclidean reflection group with degrees $d_1 \leq \cdots \leq d_\ell$ must have $d_1 = 2$ as was shown in §18-6.

Theorem A will be proved in §34-3, whereas Theorem B will be proved in §34-4.

34-2 Conjugacy classes of regular elements

In this section, preliminary to proving Theorems A and B from §34-1, we establish two propositions. In particular, the second of these will provide a necessary and

sufficient condition for two regular elements of the same order to be conjugate. Theorem A will then be proved in §34-3 by demonstrating that this condition is satisfied in the case of Weyl groups.

The propositions to be proved are extensions of results obtained in Chapter 33 and hold in the context of arbitrary pseudo-reflection groups. We shall only specialize to the case of Weyl groups when we reach the proof of Theorem A in the next section. So assume that V is a finite dimensional vector space over a *field* $\mathbb{F}$ *where* char $\mathbb{F} = 0$ and $G \subset \mathrm{GL}(V)$ is *a finite pseudo-reflection group with degrees* $\{d_1, \ldots, d_\ell\}$. Let $\varphi \in G$ be a fixed regular element of order d. It follows from Property (I-3) in §32-1 that we can choose a regular vector $x \in V$ and a primitive d-th root of unity $\xi \in \mathbb{F}$ such that

$$\varphi \cdot x = \xi x.$$

Fix choices for x and ξ. The eigenspaces $\{V(\phi, \xi)\}_{\phi \in G}$ were studied in Chapter 32. Let

$$\alpha(d) = \#\{d_i \mid d \text{ divides } d_i\}.$$

It was shown in Theorem 33-1C that

$$\max_{\phi \in G} V(\phi, \xi) = \alpha(d)$$

and, in particular, that every maximal $V(\phi, \xi)$ is of dimension $\alpha(d)$. We shall prove:

Proposition A *$V(\varphi, \xi)$ is maximal, i.e.,* $\dim V(\varphi, \xi) = \alpha(d)$.

Proof We know from Theorem 33-1C that $V(\varphi, \xi) \subset V(\phi, \xi)$ where $\dim V(\phi, \xi) = \alpha(d)$ is maximal. Since

$$\varphi \cdot x = \phi \cdot x = \xi x,$$

we have $(\varphi\phi^{-1}) \cdot x = x$. Since x is regular, $\varphi\phi^{-1} = 1$ (see Property (I-2) of §32-1). Thus $V(\varphi, \xi) = V(\phi, \xi)$. ■

We can extend Proposition A to obtain a necessary and sufficient condition for an element in G to be conjugate to φ. Given $\phi \in G$, we can show:

Proposition B *ϕ is conjugate to φ if and only if* $\dim V(\phi, \xi) = \alpha(d)$.

This proposition is an easy consequence of the next two lemmas. We know, from Theorem 33-1D, that G permutes the maximal $V(\phi, \xi)$. So in view of Proposition A, we have:

Lemma A *If* $\dim V(\phi, \xi) = \alpha(d)$, *then* $V(\phi, \xi) = \tau \cdot V(\varphi, \xi)$ *for some* $\tau \in G$.

The next lemma enables us to translate the relation $V(\phi, \xi) = \tau \cdot V(\varphi, \xi)$ into a conjugacy relation between φ and ϕ. Observe that the regularity hypothesis for x and φ is used in the proof.

Lemma B *$V(\phi, \xi) = \tau \cdot V(\varphi, \xi)$ if and only if $\tau\varphi\tau^{-1} = \phi$.*

Proof First of all, assume that $\tau\varphi\tau^{-1} = \phi$. Then

$$\tau \cdot V(\varphi, \xi) \subset V(\phi, \xi)$$

because if $\varphi \cdot y = \xi y$ then $\phi \cdot (\tau \cdot y) = \tau \cdot (\varphi \cdot y) = \xi(\tau \cdot y)$. However, the relation $\tau\varphi\tau^{-1} = \phi$ also implies that

$$\dim V(\varphi, \xi) = \dim V(\phi, \xi).$$

So the above inclusion must be an equality.

Secondly, assume $V(\phi, \xi) = \tau \cdot V(\varphi, \xi)$. In other words,

$$V(\phi, \xi) = V(\tau\varphi\tau^{-1}, \xi).$$

Thus $(\tau\varphi\tau^{-1}) \cdot x = \phi \cdot x$. Since x is regular, it follows that $\tau\varphi\tau^{-1} = \phi$. ■

Proof of Proposition B One implication is a trivial consequence of Proposition A. Conversely, suppose $\dim V(\phi, \xi) = \alpha(d)$. Then, by Lemmas A and B, ϕ is conjugate to φ. ■

Observe that the counterexample discussed in §34-1 demonstrates that regular elements of the same order in a pseudo-reflection group need not be conjugate. In particular, observe how the elements presented in that counterexample fail to satisfy the conjugacy criterion given in Proposition B.

34-3 Conjugacy classes of regular elements in Weyl groups

We now restrict to Weyl groups and prove Theorem 34-1A. We shall use the conjugacy criterion developed in §34-2 to demonstrate that regular elements of any fixed order d in a Weyl group form a single conjugacy class. As explained in §32-1, in order to determine regular elements in a Weyl group, we have to work over the complex numbers. We assume that we are dealing with a group

$$W \subset \mathrm{GL}_\ell(\mathbb{Z}) \subset \mathrm{GL}_\ell(\mathbb{C}),$$

where $W \subset \mathrm{GL}_\ell(\mathbb{C})$ is a finite pseudo-reflection group. Let $\varphi \in W$ be a regular element of order d, with $\xi \in \mathbb{C}$ a regular eigenvalue for φ. Let $\phi \in W$ be any other regular element of order d. We want to show that φ and ϕ are conjugate. By Proposition 34-2B, we need to show

$$\dim V(\phi, \xi) = \alpha(d).$$

It follows from the same type of reasoning used to establish Proposition 34-2A that there is a primitive d-th root of unity $\overline{\xi}$ such that

$$\dim V(\phi, \overline{\xi}) = \alpha(d).$$

However, there is no guarantee that $\overline{\xi} = \xi$. But it was shown in Lemma 32-4 that, since ϕ belongs to a Weyl group, each primitive d-th root of unity occurs as an eigenvalue of ϕ with the same multiplicity. In particular, $\dim V(\phi, \xi) = \dim V(\phi, \overline{\xi})$. So $\dim V(\phi, \xi) = \alpha(d)$ as desired.

34-4 Centralizers of regular elements

Let V be a finite dimensional vector space over *an algebraically closed field of characteristic zero*. Let $G \subset \mathrm{GL}(V)$ be *a finite pseudo-reflection group*. The algebraically closed hypothesis is imposed in order to ensure that Bezout's theorem can be applied. In this section, we prove Theorem 34-1B.

Let $\varphi \in G$ be a regular element. Pick a primitive d-th root of unity, ξ, which is an eigenvalue for φ. Consider the eigenvalue space

$$V(\varphi, \xi) = \{x \in V \mid \varphi \cdot x = \xi \cdot x\}.$$

It was observed in §34-1 that the centralizer $Z(\varphi) \subset G$ maps $V(\varphi, \xi)$ to itself. A stronger result actually follows from Lemma 32-2B. Namely, the property of mapping $V(\varphi, \xi)$ to itself characterizes $Z(\varphi)$. In other words:

Lemma A $Z(\varphi) = \{\phi \in G \mid \phi \cdot V(\varphi, \xi) = V(\varphi, \xi)\}$.

This characterization will be used below.

If we consider S^* and $S(V(\varphi, \xi)^*)$ as polynomial functions on V and $V(\varphi, \xi)$, respectively, then there are canonical restriction maps

$$S^* \to S\big(V(\varphi, \xi)^*\big)$$
$$R^* = S^{*G} \to S\big(V(\varphi, \xi)^*\big)^{Z(\varphi)}.$$

As in §33-4, write

$$R^* = \mathbb{F}[\omega_1, \ldots, \omega_n]$$

and arrange the $\{\omega_i\}$ so that

$$\{\omega_1, \ldots, \omega_\alpha\} \text{ have degree} \equiv 0 \pmod d$$
$$\{\omega_{\alpha+1}, \ldots, \omega_n\} \text{ have degree} \not\equiv 0 \pmod d.$$

We want to prove:

Proposition $S\big(V(\varphi, \xi)^*\big)^{Z(\varphi)} = \mathbb{F}[\omega_1, \ldots, \omega_\alpha]$.

By the results of §18-1, this proposition implies Theorem A. The proposition will follow from the next two lemmas. As in §33-4, consider the variety.

$$H(d) = \bigcap_{d_i \not\equiv 0 \pmod d} H_i, \quad \text{where } H_i = \{x \in V \mid \omega_i(x) = 0\}.$$

It can be decomposed

$$H(d) = \bigcup_{\phi \in G} V(\phi, \xi),$$

where the eigenspaces $\{V(\phi, \xi)\}$ are its irreducible components. By Proposition 34-2A, the eigenspace $V(\varphi, \xi) \subset H(d)$ is a maximal irreducible component of dimension $\alpha = \alpha(d)$. By the definition of $H(d)$,

$$\omega_{\alpha+1} = \cdots = \omega_n = 0$$

on $H(d)$ and, hence, on $V(\varphi, \xi)$. On the other hand, Lemma 33-4 tells us that $\{\omega_1, \ldots, \omega_\alpha\}$ are algebraically independent on $V(\varphi, \xi)$. Hence we have an inclusion

$$\text{(a)} \qquad \mathbb{F}[\omega_1, \ldots, \omega_\alpha] \subset S\big(V(\varphi, \xi)^*\big)^{Z(\varphi)}.$$

Moreover,

$$\text{(b)} \qquad S\big(V(\varphi, \xi)^*\big)^{Z(\varphi)} \text{ is a finite } \mathbb{F}[\omega_1, \ldots, \omega_\alpha] \text{ module.}$$

Regarding (b), observe, first of all, that, by §16-3, S^* is a finite $\mathbb{F}[\omega_1, \ldots, \omega_n]$ module. Since $S^* \to S\big(V(\varphi, \xi)^*\big)$ is surjective and since $\{\omega_{\alpha+1}, \ldots, \omega_n\}$ map to zero under this map, it follows that $\mathbb{F}[\omega_1, \ldots, \omega_\alpha] \subset S\big(V(\varphi, \xi)^*\big)$ is also finite. So the same result also holds for $\mathbb{F}[\omega_1, \ldots, \omega_\alpha] \subset S\big(V(\varphi, \xi)\big)^{Z(\varphi)}$.

It now follows from Theorem 18-4B that:

Lemma B

(i) $|Z(\varphi)|$ *divides* $\prod_{d_i \equiv 0 \ (\mathrm{mod}\ d)} d_i$;
(ii) $S\big(V(\varphi, \xi)^*\big)^{Z(\varphi)} = \mathbb{F}[\omega_1, \ldots, \omega_\alpha]$ *if and only if* $|Z(\varphi)| = \prod_{d_i \equiv 0 \ (\mathrm{mod}\ d)} d_i$.

In the rest of this section we shall prove:

Lemma C $|Z(\varphi)| = \prod_{d_i \equiv 0 \ (\mathrm{mod}\ d)} d_i$.

We pass from V to the projective space $P(V)$. This enables us to use Bezout's theorem. The hypersurfaces $H_i \subset V$ determine hypersurfaces $\overline{H_i} \subset P(V)$. Since the hypersurfaces $\{H_i\}$ intersect properly in V (see the proof of Proposition 33-1C), the hypersurfaces $\{\overline{H_i}\}$ intersect properly in $P(V)$. So we have well defined intersection multiplicities, and Bezout's theorem applies.

Bezout's Theorem *Given projective hypersurfaces that intersect properly, then the number of irreducible components of the intersection (counted with their multiplicities) equals the product of the degrees of the hypersurfaces.*

We shall work with the image

$$\overline{H(d)} = \bigcap_{d_i \not\equiv 0 \ (\mathrm{mod}\ d)} \overline{H_i}$$

in $P(V)$ of $H(d) = \bigcap_{d_i \not\equiv 0 \ (\mathrm{mod}\ d)} H_i$. By Theorem 33-1D, G acts transitively on the maximal irreducible components of

$$\overline{H(d)} = \bigcup_{\varphi \in G} \overline{V(\varphi, \xi)}.$$

So, by the characterization of $Z(\varphi)$ discussed at the beginning of this section, it follows that

$$|G|/|Z(\varphi)| = \text{the number of components of } \overline{H(d)}.$$

The transitivity of the action of G also ensures that all the components have the same multiplicity m. So Bezout's theorem tells us that

$$\prod_{d_i \not\equiv 0 \pmod{d}} d_i = m|G|/|Z(\varphi)|.$$

However, we also know that

$$|G| = \prod_i d_i.$$

Combining these identities, we have

$$|Z(\varphi)| = m \prod_{d_i \equiv 0 \pmod{d}} d_i.$$

On the other hand, by part (i) of Lemma B, we have

$$|Z(\varphi)| \leq \prod_{d_i \equiv 0 \pmod{d}} d_i.$$

It now follows that $m = 1$ and $|Z(\varphi)| = \prod_{d_i \equiv 0 \pmod{d}} d_i$. ∎

Appendices

A Rings and modules

In this appendix, we outline some basic algebra used in the book for the treatment of invariant theory. The main object of study in invariant theory is the graded invariant ring $S(V)^G$ as defined in Chapter 16. So, in particular, we need to emphasize graded analogues of classical results.

(a) Graded Rings and Algebras A *graded ring* R is a ring with a decomposition $R = \bigoplus_{j \in Z} R_j$ compatible with addition and multiplication, i.e., each R_i is an abelian group under addition, $a + b$, while multiplication, ab, consists of maps

$$R_i \times R_j \longrightarrow R_{i+j}$$

satisfying the distributive laws

$$(a+b)c = ac + bc$$
$$a(b+c) = ab + ac$$

for all $a, b, c \in R$. The ring R is said to be *associative* if $a(bc) = (ab)c$ for all $a, b, c \in R$ and *commutative* if $ab = ba$ for all $a, b \in R$. The ring R has an *identity* if there exists $1 \in R_0$ such that $1a = a1 = a$ for all $a \in R$.

The elements of R_i are said to be *homogeneous* elements of *degree i*. The compatibility of the multiplication with the grading can be restated as asserting that $\deg x = i$ and $\deg y = j$ forces $\deg xy = i + j$. We remark that a direct sum $\bigoplus_{j \in Z} R_j$ consists of all finite sums $\{a_{j_1} + \cdots + a_{j_k} \mid a_{j_s} \in R_{j_s}\}$.

Example: In this book, the canonical example of a graded ring is the polynomial algebra $A = \mathbb{F}[t_1, \ldots, t_\ell]$. For this ring, "homogeneous" and "degree" translate into the usual concepts for polynomials. For example, $\deg t_i = 1$.

Given a graded commutative ring $R = \bigoplus_{j \in Z} R_j$, a (two-sided) *graded ideal* $I \subset R$ is an ideal admitting a decomposition $I = \bigoplus_{j=0}^{\infty} I_j$, where $I_j = I \cap R_j$. A graded ideal is generated by homogeneous elements. Given a graded (two-sided) ideal $I \subset R$, then the quotient algebra R/I inherits a grading from R.

$\mathbb{F}$ will always denote a field. A *graded* $\mathbb{F}$ *algebra* is a graded associative ring $A = \bigoplus_{i \in Z} A_i$, where each A_i is an $\mathbb{F}$ vector space and the multiplication maps $A_i \times A_j \longrightarrow A_{i+j}$ are bilinear. We shall only be concerned with a specialized case of graded $\mathbb{F}$ algebras. A graded $\mathbb{F}$ algebra is *connected* if $A_i = 0$ for $i < 0$ and $A_0 = \mathbb{F}$. So we can write $A = \bigoplus_{i=0}^{\infty} A_i$. The polynomial algebra $A = \mathbb{F}[t_1, \ldots, t_\ell]$ is again the prime illustration of such an algebra. Given a connected $\mathbb{F}$ algebra A, we have the maximal ideal

$$A_+ = \bigoplus_{j \geq 1} A_j$$

where $A/A_+ = \mathbb{F}$. The identity $A_0 = \mathbb{F}$ assures that the $\mathbb{F}$ vector space structure on each A_i is given by the map $\mathbb{F} \times A_i = A_0 \times A_j \longrightarrow A_i$.

(b) Modules Modules are generalizations of vector spaces. Let R be a commutative ring with identity 1. A *(left) R module* is an abelian group M with a map $R \times M \to M$ satisfying

$$a \cdot (b \cdot x) = (ab) \cdot x$$
$$(a + b) \cdot x = a \cdot x + b \cdot x$$
$$a \cdot (x + y) = a \cdot x + b \cdot y$$
$$1 \cdot x = x$$

for all $a, b \in R$ and $x, y \in M$.

Examples:

(i) If $R = \mathbb{F}$, then the R modules consist of $\mathbb{F}$ vector spaces.
(ii) If $R = \mathbb{Z}$, then the R modules consist of abelian groups.
(iii) R is a module over itself and every ideal $I \subset R$ is a R module.
(iv) Given a subring $R \subset S$, then S is a module over R.

For R modules, there is a concept of a *submodule* $N \subset M$ and of a *direct sum* $M \oplus N$. In particular, when R is considered a module over itself, then its submodules are the ideals of R. R modules M are *free* if they have a *basis*, i.e., elements $\{x_i\}$ that span M and that are linearly independent (using coefficients in R); in other words, we can write $M = \bigoplus_i Rx_i$. In particular, vector spaces are free $\mathbb{F}$ modules. The R module M is *projective* if it is a direct summand of a free module; in other words, there exists a module M' such that $M \oplus M'$ is free. Equivalently, M is projective if, for every surjection $f \colon N \to M$ of R modules, there exists a map $g \colon M \to N$ of R modules such that $gf = 1_M$. Projective modules include free modules, but typically form a much more general class of modules. We shall see, in the proposition below, one special case wherein the two concepts agree.

A R module M is *finitely generated* if there is a finite set $\{x_1, \ldots, x_n\}$ such that every element of M is a linear combination of $\{x_1, \ldots, x_n\}$ (with coefficients in R). The R module M is *Noetherian* if every submodule is finitely generated. In particular, the ring R is Noetherian if every ideal is finitely generated. If the R module is Noetherian, then every submodule and quotient module is also Noetherian. It is a result of Hilbert that every polynomial algebra $\mathbb{F}[x_1, \ldots, x_n]$ is Noetherian. More generally, every finitely generated graded $\mathbb{F}$ algebra is Noetherian.

(c) Graded Modules Given a graded ring $R = \bigoplus_{j \in \mathbb{Z}} R_j$, then a *graded R module* is a graded abelian group $M = \bigoplus_{j \in \mathbb{Z}} M_j$, which is an R module and the action $R \times M \to M$ consists of maps

$$R_i \times M_j \to M_{i+j}$$

satisfying the same properties given in (b). In the case of a connected graded $\mathbb{F}$ algebra A, such graded modules have the property that each M_j is also an $\mathbb{F}$ vector

space (use the maps $\mathbb{F}\times M_j = A_0\times M_j \to M_j$). A *module homomorphism* $f\colon M \to N$ of graded R modules is an R linear map that preserves degrees, i.e., $f(M_i) \subset N_i$ for all i. In the case of connected graded $\mathbb{F}$ algebras, each map $f\colon M_i \to N_i$ is a map of $\mathbb{F}$ vector spaces.

The following result plays an important part in §16-4, where the Cohen-Macauley property for rings of invariants is studied.

Proposition *Let A be a graded connected commutative $\mathbb{F}$ algebra. Let M be a finitely generated graded A module. Then M is projective if and only if M is free.*

The rest of Appendix A is devoted to the proof of this proposition. We only have to prove the implication that a finitely generated projective A module is free. To do so, we need some additional machinery. For a graded module M over a graded connected $\mathbb{F}$ algebra A, we can define the *module of indecomposables*

$$Q(M) = M/A_+M.$$

Observe that $Q(M)$ is a graded $A/A_+ = \mathbb{F}$ vector space. Given M, and hence $Q(M)$, we can define the free A module

$$A \otimes_F Q(M) = \left\{\sum a_i \otimes m_i \mid a_i \in A, m_i \in Q(M)\right\},$$

where the A module structure of $A\otimes_F Q(M)$ is given by $\sum a(a_i\otimes m_i) = \sum(aa_i)\otimes m_i$. If we choose a homogeneous $\mathbb{F}$ basis of $Q(M)$ and homogeneous representatives for this basis in M, then these choices determine an embedding $Q(M) \subset M$ and an A module map

$$\varepsilon\colon A \otimes_F Q(M) \to M.$$

We shall prove the proposition by showing that, if M is finitely generated and projective, then ε is an isomorphism. Hence M is free.

A graded module $M = \bigoplus_{i\in Z} M_i$ is *bounded from below* if there exists an integer q such that $M_i = 0$ for $i \le q$. In particular, every finitely generated A module is bounded from below.

We need the following result for the proof of the proposition.

Lemma A *Let A be a graded connected F algebra and let M be a graded A module bounded from below. Then $M = 0$ if and only if $Q(M) = 0$.*

Proof We need only deal with the implication that $Q(M) = 0$ forces $M = 0$. We proceed by induction on the degree. Suppose that

$$M_i = 0 \quad \text{for } i < k.$$

We want to show that $M_k = 0$. Now $Q(M) = 0$ gives the identity $M = A_+M$. So each $x \in M_k$ can be written $x = \sum_{i\ge 1} a_i x_i$, where $a_i \in A_i$ and $x_i \in M_{k-i}$. The induction hypothesis implies that each $x_i = 0$. ∎

Lemma B *Let A be a graded connected $\mathbb{F}$ algebra and let M be a finitely generated projective graded A module. Then $\varepsilon\colon A \otimes_{\mathbb{F}} Q(M) \to M$ is an isomorphism.*

Proof The map is clearly surjective. Let $K = \operatorname{Ker} \varepsilon$. We need to show $K = 0$. Since M is projective, there exists $g\colon M \longrightarrow A \otimes_F Q(M)$ such that $\varepsilon g = 1_M$. Hence there exists a decomposition

$$(*) \qquad A \otimes_F Q(M) = K \oplus M$$

of A modules. This decomposition implies that:

(i) K is a finitely generated A module;
(ii) $Q(K) = 0$.

Regarding (i), since M is finitely generated, it follows that $Q(M)$ is a finite dimensional $\mathbb{F}$ vector space and, hence, that $A \otimes_F Q(M)$ is a finitely generated A module. As observed above $A \otimes_F Q(M)$ must be Noetherian. Thus, K is a finitely generated A module as well. Regarding (ii), since $A \otimes_F Q(M)$ and M have the same module of indecomposables, it follows from $(*)$ that $Q(K) = 0$.

It follows from (i) and (ii), along with Lemma A, that $K = 0$. ∎

B Group actions and representation theory

In all that follows, G will be a finite group. We have the concept of a *G action on a set S*, namely a map
$$G \times S \to S,$$
where each induced map $\varphi\colon S \to S$ is a permutation of S satisfying
$$e \cdot x = x$$
$$\varphi \cdot (\varphi' \cdot x) = (\varphi\varphi') \cdot x,$$
for all $x \in S$ and $\varphi, \varphi' \in G$. Here e is the identity element of G. Equivalently, we have a group homomorphism
$$\rho\colon G \to \mathrm{Perm}(S),$$
where $\mathrm{Perm}(S)$ is the permutation group of S. Given a group action $G \times S \to S$, the *G orbit* for $x \in S$ is the collection
$$\mathcal{O} = \{\varphi \cdot x \mid \varphi \in G\}.$$
G orbits provide a decomposition of S into disjoint sets.

We can also consider *G actions on vector spaces.* Let $\mathbb{F}$ be a field and V a finite dimensional vector space over $\mathbb{F}$. A G action
$$G \times V \to V$$
on V is defined as above, with the added requirement being imposed that each induced map $\varphi\colon V \to V$ is a linear isomorphism. A vector space admitting such a group action of G is also called a *G module.* We can reformulate the group action on V as a group homomorphism
$$\rho\colon G \to \mathrm{GL}(V),$$
where $\mathrm{GL}(V)$ is the general linear group of V. With this formulation, we speak of ρ as being a *representation* of G over $\mathbb{F}$.

Examples: The *trivial representation* of G is the one-dimensional representation $V = \mathbb{F}$, where $g \cdot x = x$ for all $x \in V$ and for all $g \in G$. The *regular representation* of G is the vector space with basis $\{e_g\}_{g \in G}$ and the action of G being determined by the rule
$$\varphi \cdot e_g = e_{\varphi \cdot g}.$$
A group G is said to *act trivially* on V if $g = 1$ for all $g \in G$.

G representations and G actions on sets play a significant role in this book. Pseudo-reflection groups $G \subset \mathrm{GL}(V)$ are special types of representations. This fact enables us, at times, to impose the framework of representation theory on

such groups to better understand what is happening. G actions on sets are also important in the analysis of reflection groups. Notably, Euclidean reflection groups permute their "roots" and this action plays an important role in understanding the structure of these reflection groups.

Two representations $\rho\colon G \to \mathrm{GL}(V)$ and $\rho'\colon G \to \mathrm{GL}(V')$ are *isomorphic* if there is a linear isomorphism $f\colon V \to V'$ so that the following diagram commutes.

$$\begin{tikzcd} G \arrow[r, "\rho"] \arrow[dr, "\rho'"'] & \mathrm{GL}(V) \arrow[d, "f(-)f^{-1}"] \\ & \mathrm{GL}(V') \end{tikzcd}$$

We do not distinguish between isomorphic representations.

We can reformulate the above in terms of G modules. Given G modules V, V', a *G-equivariant map* $f\colon V \to V'$ is a $\mathbb{F}$ linear map such that, for all $\varphi \in G$, the following diagram commutes

$$\begin{tikzcd} V \arrow[r, "f"] \arrow[d, "\varphi"] & V' \arrow[d, "\varphi"] \\ V \arrow[r, "f"] & V' \end{tikzcd}$$

We say that two G modules V and V' are *isomorphic* if there exists a G-equivariant linear isomorphism $f\colon V \xrightarrow{\cong} V'$. G modules classified up to isomorphism are the same as representations classified up to isomorphism.

(1) Reducible and Completely Reducible Given a G module V, a subspace $V' \subset V$ is *stable* under G if each $\varphi \in G$ maps V' to itself. (Such a subspace is also commonly described as being *invariant* under G. To avoid confusion, we limit the use of that term to the case where elements are pointwise fixed under the action of G.) A representation $\rho\colon G \to \mathrm{GL}(V)$ is *irreducible* if $V \neq 0$ and the only G-stable subspaces of V are 0 and V. Otherwise, a representation is said to be *reducible.* In this latter case a stronger property often holds. A representation $\rho\colon G \to \mathrm{GL}(V)$ is *completely reducible* if, given $V' \subset V$ stable under G, there exists $V'' \subset V$ also stable under G such that $V = V' \oplus V''$. This is the same as saying that we can write $\rho = \rho' \oplus \rho''$, a direct sum of the representations

$$\rho' G \to \mathrm{GL}(V')$$
$$\rho''\colon G \to \mathrm{GL}(V'').$$

Representation theory naturally divides into the modular and nonmodular cases. The *modular case* is when $\operatorname{char}\mathbb{F}$ divides $|G|$, i.e., $\operatorname{char}\mathbb{F} = p > 0$ and p divides $|G|$. The *nonmodular case* is when $\operatorname{char}\mathbb{F}$ does not divide $|G|$. In particular, this includes the case $\operatorname{char}\mathbb{F} = 0$. Considerably more is known about the nonmodular case. Notably, in this case *averaging* (as defined in §13-3) can be

carried out. The main result with regards to complete reducibility is Maschke's Theorem. It holds in the nonmodular case, and its proof illustrates the usefulness of averaging.

Maschke's Theorem *If* char $\mathbb{F}$ *does not divide* $|G|$, *then every representation* $\rho\colon G \to \mathrm{GL}(V)$ *over* $\mathbb{F}$ *is completely reducible.*

Proof Suppose we have $U \subset V$ stable under G. Choose a vector space projection $q\colon V \to V$ with $\operatorname{Im} q = U$. There are many choices for q. Choosing q is the same as picking a vector space complement ($= \operatorname{Ker} q$) to U. We want to find a complement that is stable under G. Equivalently, we want to choose q to be G-equivariant, i.e.,

$$\phi \cdot q(x) = q(\phi \cdot x) \quad \text{for all } \phi \in G \text{ and } x \in V.$$

Given an arbitrary projection q, we can modify it to obtain the G-equivariant property. Namely, let

$$\widehat{q} = \frac{1}{|G|} \sum_{\varphi \in G} \varphi^{-1} q \varphi.$$

(i) $\widehat{q}$ is G-equivariant.

We have the identities

$$\widehat{q}(\phi \cdot x) = \frac{1}{|G|} \sum_{\varphi \in G} \varphi^{-1} \cdot q(\varphi \cdot \phi \cdot x) = \phi \frac{1}{|G|} \sum_{\varphi \in G} (\varphi\phi)^{-1} q\big((\varphi\phi) \cdot x\big) = \phi \cdot \widehat{q}(x).$$

(ii) $\operatorname{Im} \widehat{q} = U$.

The fact that $\operatorname{Im} \widehat{q} \subset U$ follows from the definition of $\widehat{q}$ and the fact that U is stable. The fact that $\widehat{q}\colon V \to U$ is surjective follows from the fact that $U \subset V \xrightarrow{\widehat{q}} U$ is the identity.

It follows from (i) and (ii) that $\operatorname{Ker} \widehat{q}$ is a complement to U and invariant under G. ∎

Under the nonmodular hypothesis, we can continue the above decomposition process until each constituent representation is irreducible. So, in the nonmodular case, every representation can be decomposed into a direct sum of irreducible representations. There is only a finite number of irreducible $\mathbb{F}$ representations $W_1, \ldots, W_k$ of G and every $\mathbb{F}$ representation of G has an unique decomposition

$$\rho \cong \sum_{i=1}^{k} n_i W_i$$

in terms of these irreducible representations. We remark that the individual summands isomorphic to some W_i are not uniquely determined, but each collected summand

$$n_i W_i = W_i \oplus \cdots \oplus W_i$$

comprising all isomorphic copies of a particular W_i is unique.

Example: In the nonmodular case, the regular representation R has a decomposition $R \cong \sum_{i=1}^{k} d_i W_i$, where $W_1, \ldots, W_k$ are all the irreducible representations and $d_i = \dim_{\mathbb{F}} W_i$.

(2) ***Characters*** Representations are usually studied through their associated characters. Given a representation $\rho\colon G \to \mathrm{GL}(V)$, then we define its associated character $\chi\colon G \to \mathbb{F}$ by

$$\chi(g) = \mathrm{tr}\big(\rho(g)\big),$$

where $\mathrm{tr}(\varphi)$ denotes the trace of the linear transformation $\varphi\colon V \to V$. Characters are *class functions*, i.e.,

$$\chi(\varphi^{-1} g \varphi) = \chi(g) \quad \text{for all } g, \varphi \in G.$$

Example: The character of the trivial representation of G is given by $\chi(g) = 1$ for all $g \in G$. The character of the regular representation of G is given by

$$\chi(g) = \begin{cases} |G| & \text{if } g = e \\ 0 & \text{if } g \neq e. \end{cases}$$

An elemental fact of representation theory is that, in the nonmodular case, each representation is uniquely determined by its character. If $\{\omega_1, \ldots, \omega_k\}$ are the characters of the irreducible representations $W_1, \ldots, W_k$, then they are linearly independent class functions and

$$\rho \cong \sum_{i=1}^{k} n_i W_i \quad \text{if and only if } \chi = \sum_{i=1}^{k} n_i \omega_i.$$

We can define an inner product $(\_, \_)$ on the vector space of class functions by the rule

$$(\chi, \lambda) = \frac{1}{|G|} \sum_{\varphi \in G} \chi(\varphi) \lambda(\varphi)^{-1}.$$

Then $\{\omega_1, \ldots, \omega_k\}$ are orthonormal, i.e., $(\omega_i, \omega_j) = \delta_{ij}$. Also, the inner product gives the coefficients of $\{\omega_1, \ldots, \omega_k\}$ in the above expansions. Namely, if $\chi = \sum_{i=1}^{k} n_i \omega_i$, then $n_i = (\chi, \omega_i)$.

(3) ***Fields of Definition*** The representations of G depend upon the field over which we are working. For example, if $G = \mathbb{Z}/n\mathbb{Z}$ is generated by φ and $V = \mathbb{F}$, then the action of G on V given by

$$\varphi \cdot x = \zeta x, \quad \text{where } \zeta = \text{the } n\text{-th root of unity}$$

only makes sense if $\zeta \in \mathbb{F}$. This example illustrates that, as we move to larger fields, the number of possible representations increases. Given a field extension $\mathbb{F} \subset \mathbb{F}'$, then all the representations over $\mathbb{F}$ can be regarded as representations over $\mathbb{F}'$ (by linear extension), but there may also be new representations defined over $\mathbb{F}'$ that are not defined over $\mathbb{F}$. In particular, new irreducible representations may arise and an irreducible representation over $\mathbb{F}$ may turn out to be decomposable over $\mathbb{F}'$ by using these new representations.

Example: The rotation $\varphi = \begin{bmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{bmatrix}$ of the Euclidean plane through the angle $2\pi/n$ can be diagonalized over $\mathbb{C}$, namely $\varphi = \begin{bmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{bmatrix}$, where ζ is as above. This example provides a two-dimensional rotation representation of $G = \mathbb{Z}/n\mathbb{Z}$ irreducible over $\mathbb{R}$, but decomposing over $\mathbb{C}$ as a sum of two (one-dimensional) representations.

When fields are *sufficiently large*, the representations of G stabilize. First of all, we observe that there is a procedure for identifying representations over different fields. We have already noted this in the case of an inclusion $\mathbb{F} \subset \mathbb{F}'$. If there is not an inclusion $\mathbb{F} \subset \mathbb{F}'$, we pass to the *composite field* $k = \mathbb{F}\mathbb{F}'$ and use the inclusions $\mathbb{F} \subset k$ and $\mathbb{F}' \subset k$ to convert all representations into k representations. We then check to see when these k representations are isomorphic.

The above type of identifications enormously simplify the total collection of representations of G. It is a finite collection and is realized over any sufficiently large enough field. Namely, given any $\mathbb{F}$, we can find an extension $\mathbb{F} \subset \mathbb{F}'$ such that all representations of G are defined over $\mathbb{F}'$. In particular, Brauer proved that all the representations of G are defined over any field containing the $|G|$-th roots of unity.

As an illustration of why we need to pay attention to the field of definition, the following is used in Chapter 31 and demonstrates the advantages of working over algebraically closed fields.

Schur's Lemma: *Let $\mathbb{F}$ be an algebraically closed field and let $\rho\colon G \to \mathrm{GL}(V)$ be an irreducible representation over F. Then every element of $Z(G)$ acts on V as scalar multiplication by some $\lambda \in \mathbb{F}$.*

Proof Let $\tau \in Z(G)$. For each $\xi \in \mathbb{F}$, let

$$V(\tau, \xi) = \{x \in V \mid \tau \cdot x = \xi x\}$$

be the eigenspace corresponding to ξ. $\mathbb{F}$ algebraically closed guarantees that τ is diagonalizable, i.e., V is a direct sum of the spaces $\{V(\tau, \xi)\}$. Moreover, G maps each $V(\tau, \xi)$ to itself. For, given $x \in V(\tau, \xi)$ and $\varphi \in G$, then

$$\tau \cdot (\varphi \cdot x) = \varphi \cdot (\tau \cdot x) = \xi(\varphi \cdot x).$$

So $\varphi \cdot x \in V(\tau, \xi)$. It follows that there cannot be two distinct eigenspaces of τ. Otherwise, G would not act irreducibly on V. ∎

At the other end of the spectrum, we are often interested in the smallest field over which a reflection can be defined. A representation $\rho\colon G \to GL_n(\mathbb{F})$ is *defined over the subfield* $\mathbb{F}' \subset \mathbb{F}$ if it arises (via linear extension) from a representation $\rho'\colon G \to GL_n(\mathbb{F}')$. Let $\chi\colon G \to \mathbb{F}^*$ be the character of ρ and assume that char $\mathbb{F} = 0$. In particular, we have $\mathbb{Q} \subset \mathbb{F}$.

Definition: The *character field* $\mathbb{Q}(\chi)$ is the extension of $\mathbb{Q}$ generated by $\operatorname{Im}\chi \subset \mathbb{F}^*$.

By the definition of $\mathbb{Q}(\chi)$, we can have $\rho\colon G \to GL_n(\mathbb{F})$ defined over $\mathbb{F}' \subset \mathbb{F}$ only if $\mathbb{Q}(\chi) \subset \mathbb{F}'$. But this condition is usually not sufficient. An arbitrary representation $\rho\colon G \to GL_n(\mathbb{F})$ with character χ is usually not defined over $\mathbb{Q}(\chi)$ itself, only over a finite extension of $\mathbb{Q}(\chi)$. The Schur index measures how far ρ deviates from being defined over $\mathbb{Q}(\chi)$. To simplify notation, let

$$\mathbb{K} = \mathbb{Q}(\chi).$$

Let m be the minimal integer such that $m\rho$ (direct sum of ρ) is defined over $\mathbb{K}$. Such an integer exists and is called the *Schur index*). We now explain how to obtain m. The group ring $\mathbb{K}[G]$ (see §13-1) decomposes into irreducible factors

$$\mathbb{K}[G] = \Lambda_1 \times \cdots \times \Lambda_r.$$

(This is just a different formulation of Maschke's Theorem.) The character map $\chi\colon G \to \mathbb{F}$ associated with ρ extends to a map $\chi\colon \mathbb{K}[G] \to \mathbb{F}$ and, since ρ is irreducible, χ is nonzero on only one of the factors. Call this factor Λ. We can write

$$\Lambda = M_{k\times k}(D),$$

where D is a division ring of dimension m^2 over $\mathbb{K}$. We then have $n = km$. Moreover, the representation $m\rho$ can be obtained from Λ. Let

$I =$ the elements of $M_{k\times k}(D)$, which are trivial except in the final column.

The map $\pi\colon G \to \mathbb{K}[G] \to \Lambda$ gives an action of G on I and $\pi = m\rho$. For more about the above, consult Curtis-Reiner [1] and Lam [1].

We can use the Schur index to prove the following lemma, which is used in §15-2.

Lemma *If ρ is an irreducible representation and $\rho(G) \subset GL_n(\mathbb{F})$ contains a pseudo-reflection, then ρ is defined over $\mathbb{Q}(\chi)$.*

Proof We shall continue to use the above notation. To show $m = 1$, pick $\varphi \in G$ such that $\rho(\varphi)$ is a pseudo-reflection. First of all, $\dim_D I^{\pi(\varphi)} \leq k - 1$ tells us that

$$(*) \qquad \dim_K I^{\pi(\varphi)} \leq m^2(k-1) = m(n-m).$$

On the other hand, the fact that $\pi = m\rho$, and that $\rho(\varphi)$ leaves a hyperplane of dimension $n-1$ pointwise invariant, tells us that

$$(**) \qquad m(n-1) \leq \dim_K I^{\pi(\varphi)}.$$

Combining $(*)$ and $(**)$ we have $m = 1$. ■

(4) Stable Isomorphisms It has already been observed that representation theory incorporates the theory of pseudo-reflection groups. Pseudo-reflection groups $G \subset \mathrm{GL}(V)$ can be thought of as *(pseudo) reflection representations* $\rho\colon G \to \mathrm{GL}(V)$. Thinking of reflection groups in this context, we use the rest of the appendix to discuss the idea of stable isomorphisms of reflection groups. This concept of stable isomorphism is needed in §5-3 and, more generally, for the classification results for Euclidean reflection groups obtained in Chapter 7.

Let $\rho\colon G \to \mathrm{GL}(V)$ be a (pseudo) reflection representation over a field $\mathbb{F}$, where $\operatorname{char}\mathbb{F}$ does not divide $|G|$). Then Maschke's theorem applies and ρ is completely reducible. We now demonstrate that, when we write ρ as a sum of irreducible representations, then the irreducible components are:

(i) reflection representations;
(ii) trivial representations.

No other representations arise as components. To see this, write $V = V_1 \oplus \cdots \oplus V_k$, where each V_i is invariant under the action of G. Pick a pseudo-reflection $s\colon V \to V$ of order n and $\alpha \in V$, where $s \cdot \alpha = \zeta\alpha$ where ζ is a primitive n-th root of unity. We want to show that $\alpha \in V_i$ for some i. Write

$$\alpha = \alpha_1 + \cdots + \alpha_k,$$

where $\alpha_i \in V_i$. Then $s \cdot \alpha_i = \zeta\alpha_i$ for each i. Since $\operatorname{rank}(1-s) = 1$, it follows that $\alpha_i \neq 0$ for only one i. Thus, $\alpha = \alpha_i \in V_i$.

The above observations lead to the concept of a stable isomorphism. Two reflection representations $\rho\colon G \to \mathrm{GL}(V)$ and $\rho'\colon G \to \mathrm{GL}(V')$ will be said to be *stably isomorphic* if $\rho \oplus \tau \cong \rho' \oplus \tau'$, where τ and τ' each consist of a finite number of copies of the trivial representation. In §2-3, the idea of essential root systems and essential Euclidean reflection groups were introduced. As pointed out there, every Euclidean reflection group is stably isomorphic to an essential one. So there is a one-to-one correspondence:

$$\left\{\begin{matrix}\text{stable isomorphism classes of}\\ \text{finite Euclidean reflection groups}\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{isomorphism classes of finite}\\ \text{essential Euclidean reflection}\\ \text{groups}\end{matrix}\right\}.$$

This fact is relevant to the discussions of §5-2 and §5-3.

C Quadratic forms

In all that follows, V will denote a finite dimensional real vector space. In this appendix, we shall establish some facts concerning bilinear forms

$$\mathcal{B}\colon V \times V \to \mathbb{R}$$

and their associated quadratic forms

$$q\colon V \to \mathbb{R}$$
$$q(x) = \mathcal{B}(x, x).$$

We point out that we can recover $\mathcal{B}$ from q by the rule

$$\mathcal{B}(x, y) = \frac{1}{2}[q(x + y) - q(x) - q(y)].$$

A *quadratic form* is defined to be a map $q\colon V \to \mathbb{R}$ such that the right-hand side of the above expression giving $\mathcal{B}(x, y)$ is bilinear. So, by definition, there is a one-to-one correspondence between bilinear forms and quadratic forms on V. A bilinear form is *symmetric* if $\mathcal{B}(x, y) = \mathcal{B}(y, x)$ for all $x, y \in V$. A bilinear form is *nondegenerate* if and only if

$$V^{\perp} = \{x \in V \mid \mathcal{B}(x, y) = 0 \text{ for all } y \in V\}$$

is trivial. A bilinear form is *nonnegative* if $\mathcal{B}(x, x) \geq 0$ for all $x \in V$ and *positive definite* if $\mathcal{B}(x, x) > 0$ for all $0 \neq x \in V$. Given a basis S of V, a bilinear form is *reducible* with respect to S if we can partition S into two nontrivial sets $S = S_1 \coprod S_2$ so that $\mathcal{B}(x, y) = 0$ if $x \in S_1$ and $y \in S_2$. Otherwise, it is said to be *irreducible* with respect to S.

Bilinear forms and their associated quadratic forms can be represented by matrices. Given an (ordered) basis $\{e_1, \ldots, e_\ell\}$ of V, then

$$A = [\mathcal{B}(e_i, e_j)]_{\ell \times \ell}$$

is a *representing matrix* of $\mathcal{B}$ or q. If $x = \sum_{i=1}^{\ell} x_i e_i$ and $y = \sum_{i=1}^{\ell} y_i e_i$, then

$$\begin{aligned} \mathcal{B}(x, y) &= X^t A Y \\ q(x) &= X^t A X \end{aligned} \quad \text{where} \quad X = \begin{bmatrix} x_1 \\ \vdots \\ x_\ell \end{bmatrix} \text{ and } Y = \begin{bmatrix} y_1 \\ \vdots \\ y_\ell \end{bmatrix}.$$

The various representing matrices of a bilinear form $\mathcal{B}$ are related. Namely, if A and A' are the representing matrices of $\mathcal{B}$ with respect to the bases $\{e_1, \ldots, e_\ell\}$ and $\{e'_1, \ldots, e'_\ell\}$, then

$$A' = T^t A T,$$

where T is the transitional matrix between the two bases, namely $Te_j = \sum_{i=1}^{\ell} T_{ij}e_i'$.

Given a bilinear form, we would like to choose a basis so that the representing matrix is as simple as possible. Clearly, a matrix A representing a bilinear form $\mathcal{B}$ is always symmetric if $\mathcal{B}$ is symmetric. Even more, if $\mathcal{B}$ is symmetric, we can always choose a basis such that the representing matrix is diagonal. Equivalently, for any symmetric matrix there exists a (orthogonal) matrix T such that $TAT^{-1} = TAT^t$ is diagonal. (See, for example, §10-2 of Hoffman-Kunze [1] for justifications of these assertions.)

The first goal of this appendix will be to prove a result concerning the kernel of certain quadratic forms. Given $q\colon V \to \mathbb{R}$, let

$$\operatorname{Ker} q = \{x \in V \mid q(x) = 0\}.$$

We shall prove:

Proposition A *Suppose* $\mathcal{B}\colon V \times V \to \mathbb{R}$ *is a nonnegative, symmetric bilinear form. Suppose* $\mathcal{B}$ *is irreducible with respect to the basis* $\{e_1, \ldots, e_\ell\}$ *and* $\mathcal{B}(e_i, e_j) \le 0$ *for* $i \ne j$. *If* $\operatorname{Ker} q \ne 0$, *then* $\operatorname{Ker} q$ *contains an element having positive coefficients with respect to* $\{e_1, \ldots, e_\ell\}$.

This result can be reformulated in terms of the representing matrices of $\mathcal{B}$ and q. It is this matrix version, or more exactly a corollary of it, that will be needed for the study of Coxeter elements in Chapter 29. We first have to introduce some concepts. In view of the correspondence between forms and matrices, we shall also say that an $\ell \times \ell$ matrix $A = [a_{ij}]$ is *nonnegative* if $X^tAX \ge 0$ for all column vectors X and *irreducible* if we cannot partition the set $\{1, 2, \ldots, \ell\}$ into two nonempty sets S_1 and S_2 such that $a_{ij} = 0$ when $i \in S_1$ and $j \in S_2$. So a matrix A representing a bilinear form B with respect to a basis S is nonnegative (or irreducible) if $\mathcal{B}$ is nonnegative (or irreducible with respect to S). In analogue to Proposition A, we have:

Proposition B *Let* $A = [a_{ij}]_{\ell \times \ell}$ *be a real symmetric, nonnegative, irreducible matrix such that* $a_{ij} \le 0$ *for* $i \ne j$. *If* $\operatorname{Ker} A \ne 0$, *then* $\operatorname{Ker} A$ *contains a vector with all positive entries.*

Propositions A and B are equivalent. Think of A as being the representing matrix of $\mathcal{B}$ and q. Then the equivalence of the propositions follows from

$$(*) \qquad X^tAX = 0 \quad \text{if and only if } AX = 0.$$

(Here we are using the notation introduced previously.) As regards $(*)$, it is true if A is diagonal. Next, consider an arbitrary symmetric A. As already observed, there exists an orthogonal matrix T such that $TAT^t = TAT^{-1}$ is diagonal. So the equivalence $(*)$ holds for TAT^t and we can use that fact to deduce that $(*)$ holds A. Namely $(TX)^t(TAT^t)TX = X^tAX = 0$ implies that $TAX = (TAT^t)TX = 0$, and hence that $AX = 0$.

Proof of Proposition A Suppose $\operatorname{Ker} q \ne 0$.

(i) $q(\sum_{i=1}^{\ell} c_i e_i) = 0$ implies $q(\sum_{i=1}^{\ell} |c_i| e_i) = 0$.

This follows from the series of inequalities

$$0 \le q\Big(\sum_{i=1}^{\ell} |c_i| e_i\Big) = \sum_{i,j} |c_i|\,|c_j| \mathcal{B}(e_i, e_j) \le \sum_{i,j} c_i c_j \mathcal{B}(e_i, e_j) = q\Big(\sum_{i=1}^{\ell} c_i e_i\Big) = 0.$$

The middle inequality uses the fact that $\mathcal{B}(e_i, e_j) \le 0$ for $i \ne j$. Let

$$q_{ij} = \mathcal{B}(e_i, e_j).$$

(ii) $q(\sum_{i=1}^{\ell} |c_i| e_i) = 0$ implies $\sum_{i=1}^{\ell} |c_i| q_{ij} = 0$ for each j.

To prove (ii), we translate $q(x)$ into matrix form. If $x = \sum_{i=1}^{\ell} x_i e_i$, then

$$(**) \qquad q(x) = X^t Q X, \quad \text{where } Q = [q_{ij}] \text{ and } X = \begin{bmatrix} x_1 \\ \vdots \\ x_\ell \end{bmatrix}.$$

Moreover, it follows from $(*)$ that

$$(***) \qquad X^t Q X = 0 \quad \text{if and only if } X^t Q = 0.$$

(Since Q is symmetric, we have $(QX)^t = X^t Q$. So $QX = 0$ if and only if $X^t Q = 0$.) If we combine $(**)$ and $(***)$ for $x = \sum_{i=1}^{\ell} |c_i| e_i$, then (ii) follows

(iii) $c_k \ne 0$ for each k.

To see this, let

$$I = \{i \mid c_i \ne 0\} \quad \text{and} \quad J = \{i \mid c_i = 0\}.$$

We want to show $J = \varnothing$. The fact that $\operatorname{Ker} q \ne 0$ means that we can assume $I \ne \varnothing$. We shall show that $q_{ij} = 0$ if $i \in I$ and $j \in J$. The irreducibility of $\mathcal{B}(x, y)$ then forces $J = \varnothing$. For any j, the equation $\sum_{i=1}^{\ell} |c_i| q_{ij} = 0$ from (ii) can be simplified to $\sum_{i \in I} |c_i| q_{ij} = 0$. Since $j \in J$, we have $q_{ij} \le 0$ for all $i \in I$ (for we have $i \ne j$). Consequently $q_{ij} = 0$.

Lastly, if we combine (i), (ii) and (iii) then the proposition follows. ■

We notice a consequence of Proposition B, which will be used in the study of Coxeter elements in Chapter 28.

Corollary A *Let $A = [a_{ij}]_{\ell \times \ell}$ be a real, symmetric, nonnegative, irreducible matrix such that $a_{ij} \le 0$ for $i \ne j$. Then A has an eigenvector with all positive entries.*

Proof We shall show that, for some $\lambda \in \mathbb{R}$, $A - \lambda I$ satisfies the hypothesis, and hence the conclusion, of Proposition B. Since A is real and symmetric, it can be diagonalized; more exactly, we can find an orthogonal matrix T such that $TAT^{-1} = TAT^t$ is diagonal. In particular, the diagonal terms are real. Since TAT^t is also nonnegative, the diagonal terms of TAT^t must be nonnegative. Let λ be the minimal diagonal term. Then $A - \lambda I = [b_{ij}]_{\ell \times \ell}$ is a real, symmetric, nonnegative, irreducible matrix such that $b_{ij} \leq 0$ for $i \neq j$. Moreover, $\mathrm{Ker}(A - \lambda I) \neq 0$. We conclude from Proposition B that $\mathrm{Ker}(A - \lambda I)$ has a vector with all positive entries. ∎

We next study bilinear and quadratic forms on real vector spaces admitting an action of a finite group. Given a vector space V, then, as pointed out in Appendix B, specifying an action $G \times V \longrightarrow V$ of a finite group G on V is equivalent to specifying a representation $\rho \colon G \longrightarrow \mathrm{GL}(V)$. Given an action of G on V, we are interested in *G-invariant forms.* These are bilinear forms $\mathcal{B} \colon V \times V \longrightarrow \mathbb{R}$ and quadratic forms $q \colon V \longrightarrow \mathbb{R}$ satisfying

$$\mathcal{B}(\varphi \cdot x, \varphi \cdot y) = \mathcal{B}(x, y) \quad \text{and} \quad q(\varphi \cdot x) = q(x)$$

for all $\varphi \in G$, $x, y \in V$. The one-to-one correspondence between bilinear and quadratic forms passes to those that are G-invariant.

We can easily produce a G-invariant bilinear form that is both symmetric and positive definite (i.e., an inner product). Just take any positive definite form $\mathcal{B}'$ and average it to obtain $\widehat{\mathcal{B}}$

$$\widehat{\mathcal{B}}(x, y) = \sum_{\varphi \in G} \mathcal{B}'(\varphi \cdot x, \varphi \cdot y).$$

Under suitable hypotheses, we can also obtain uniqueness results for G-invariant forms: any two choices differ by a scalar multiple. So, in these circumstances, any G-invariant bilinear form must be a multiple of $\widehat{\mathcal{B}}$. The main result is:

Proposition C *Let G be a finite group. Let $\rho \colon G \longrightarrow \mathrm{GL}(V)$ be an irreducible representation. Any nontrivial G-invariant bilinear form $\mathcal{B} \colon V \times V \longrightarrow \mathbb{R}$ is nondegenerate.*

Proof We want to show that $V^{\perp} = 0$. Observe that $\mathcal{B} \neq 0$ implies $V^{\perp} \neq V$. Next, $V^{\perp}$ is stable under G. Consider $x \in V^{\perp}$. For all $y \in V$ and $\varphi \in G$, we have the identities

$$\mathcal{B}(\varphi \cdot x, y) = \mathcal{B}(x, \varphi^{-1} \cdot y) = 0.$$

By the irreducibility of ρ, $V^{\perp} = 0$. ∎

As defined in Chapter 14, a *reflection* on a real vector space V is a linear transformation $s \colon V \longrightarrow V$ that leaves a hyperplane $H \subset V$ pointwise fixed and acts as multiplication by -1 on a complementary line L.

Proposition D *Let G be a finite group. Let $\rho \colon G \longrightarrow \mathrm{GL}(V)$ be an irreducible representation. Suppose the subgroup $\mathrm{Im}\, \rho \subset \mathrm{GL}(V)$ contains a reflection. Then any two G-invariant nondegenerate bilinear forms on V are multiples of each other.*

Proof Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be the bilinear forms on V. Their nondegeneracy gives isomorphisms

$$f_1 : V \xrightarrow{\cong} V^*$$
$$f_2 : V \xrightarrow{\cong} V^*.$$

Just pick any $0 \neq \alpha \in V$ and let $f_1(\_) = \mathcal{B}_1(\alpha, \_)$ and $f_2(\_) = \mathcal{B}_2(\alpha, \_)$. These isomorphisms, in turn, give an isomorphism

$$\Phi = f_2^{-1} f_1 : V \xrightarrow{\cong} V,$$

which is set up to satisfy the identity

$$\mathcal{B}_1(x, y) = \mathcal{B}_2\big(\Phi(x), y\big) \quad \text{for all } x, y \in V.$$

(Since we have $f_2\big(f_2^{-1} f_1(x)\big) = f_1(x)$.) So, to prove $\mathcal{B}_1$ and $\mathcal{B}_2$ are multiples of each other, it suffices to show Φ is multiplication by some k.

(i) Φ is G-equivariant.

Pick $x \in V$ and $\varphi \in G$. Then

$$\begin{aligned} \mathcal{B}_2\big(\Phi(\varphi \cdot x), y\big) &= \mathcal{B}_1(\varphi \cdot x, y) = \mathcal{B}_1(x, \varphi^{-1} \cdot y) \\ &= \mathcal{B}_2\big(\Phi(x), \varphi^{-1} \cdot y\big) = \mathcal{B}_2\big(\varphi \cdot \Phi(x), y\big). \end{aligned}$$

Since the above identities hold for all $y \in V$, and since $\mathcal{B}_2$ is nondegenerate, we must have $\Phi(\varphi \cdot x) = \varphi \cdot \Phi(x)$.

(ii) $\Phi(\alpha) = k\alpha$ for some $k \in \mathbb{R}$ and $\alpha \in V$.

Choose a reflection $s_\alpha : V \to V$ from $\operatorname{Im} \rho \subset \mathrm{GL}(V)$. So $s_\alpha \cdot \alpha = -\alpha$ while $s_\alpha|_H = \mathrm{id}$ for some hyperplane $H \subset V$. By (i), we have $s_\alpha \cdot \Phi(\alpha) = \Phi(s_\alpha \cdot x) = -\Phi(\alpha)$. Consequently, $\Phi(\alpha)$ is a multiple of α because $\mathbb{F}\alpha$ is the eigenvalue space on which $s_\alpha = -1$.

(iii) $\operatorname{Ker}(\Phi - k) = V$.

By (i) and (ii), we know that $\operatorname{Ker}(\Phi - k) \neq 0$ and is invariant under G. Now use the fact that $\rho : G \to \mathrm{GL}(V)$ is irreducible. ■

It follows from the previous two propositions that any nontrivial, G-invariant bilinear form is of the form $k\widehat{\mathcal{B}}$. To determine k, we need only compare $\mathcal{B}(x, x)$ and $\widehat{\mathcal{B}}(x, x)$ for any point $x \in V$.

In view of the correspondence between G-invariant bilinear and quadratic forms, we can use the above propositions to deduce:

Corollary B *Let G be a finite group. Let $\rho : G \to \mathrm{GL}(V)$ be an irreducible representation. Suppose the subgroup $\operatorname{Im} \rho \subset \mathrm{GL}(V)$ contains a reflection. Then any two nontrivial G-invariant quadratic forms on V are multiples of each other.*

D Lie algebras

The relation between crystallographic root systems and Lie algebras is quite direct. What follows is a very brief sketch of that relation. For more details, and in particular for undefined terms, the reader is referred to any standard book on Lie algebras (e.g. Humphreys [1]).

Let L be a finite dimensional semi-simple Lie algebra over $\mathbb{C}$ with bracket product $[\_, \_]$. Choose a Cartan subalgebra $H \subset L$. Such subalgebras are unique up to automorphisms of L and also have the property of being maximal abelian subalgebras (i.e., $[x, y] = 0$ for all $x, y \in L$). For each $h \in H$, we have an action on L given by the Lie bracket product.

$$\mathrm{ad}(h)\colon L \longrightarrow L$$
$$\mathrm{ad}(h)(x) = [h, x].$$

Since H is abelian, the linear transformations $\{\mathrm{ad}(h) \mid h \in H\}$ are simultaneously diagonalizable. So we can decompose

$$L = \bigoplus_{\alpha \in H^*} L_\alpha,$$

where the elements of each L_α are eigenvectors for all the elements of H and the linear functional $\alpha\colon H \longrightarrow \mathbb{C}$ gives the eigenvalue for each element of H. That is,

$$\mathrm{ad}(h)(x) = \alpha(h)x$$

for each $h \in H$ and $x \in L_\alpha$. Because of the maximality of H, we have $L_0 = H$. So we can refine the above decomposition and write it as

$$L = H \oplus \left[\bigoplus_{\alpha \in \Delta} L_\alpha\right],$$

where $\Delta \subset H^*$ is a finite set of nonzero vectors and $L_\alpha \neq 0$ for each $\alpha \in \Delta$. The collection Δ is an essential crystallographic root system as defined in Chapter 2. In particular, although H^* is a complex vector space, we can locate a Euclidean space $\mathbb{E} \subset H^*$ (of the same dimension) so that $\Delta \subset \mathbb{E}$.

There is actually a one-to-one correspondence between essential crystallographic root systems and finite dimensional semi-simple Lie algebras over $\mathbb{C}$. The above discussion provides the first half of the relation, namely an explanation of how to associate a root system to a Lie algebra. Serre's Theorem provides the other half of the relation.

Serre's Theorem Serre's Theorem is based on the observation that the root system Δ associated with the Lie algebra L is more than just an index set for decomposing L; Δ actually contains enough information to completely determine L as a Lie algebra.

The root system has a simple relation to multiplication in the Lie algebra. Given $\alpha, \beta \in \Delta$, we have

$$[L_\alpha, L_\beta] = \begin{cases} L_{\alpha+\beta} & \text{if } \alpha+\beta \in \Delta \\ 0 & \text{if } \alpha+\beta \notin \Delta \end{cases}$$

(this includes the case $L_0 = H$). Moreover, this rule can be considerably refined. From the discussion of crystallographic root systems in Chapters 8 and 9, the crystallographic root system is determined up to isomorphism by choosing a fundamental system $\{\alpha_1, \dots, \alpha_\ell\}$ and calculating the integers $\langle \alpha_i, \alpha_j \rangle \in \mathbb{Z}$ as defined in §9-1. Serre's Theorem explains how we can use any such fundamental system and its associated integers to also define the algebra L. We have $\dim L_\alpha = 1$ for each $\alpha \in \Delta$, and we can choose nonzero elements

$$h_i \in H, \quad x_i \in L_{\alpha_i} \quad \text{and} \quad y_i \in L_{-\alpha_i} \quad \text{for } 1 \le i \le \ell$$

satisfying the relations

(i) $[h_i, h_j] = 0$;

(ii) $[x_i, y_j] = \begin{cases} h_i & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$;

(iii) $[h_i, x_j] = \langle \alpha_j, \alpha_i \rangle x_j$;

(iv) $[h_i, y_j] = -\langle \alpha_j, \alpha_i \rangle y_j$;

(v) $\mathrm{ad}(x_i)^{-\langle \alpha_j, \alpha_i \rangle + 1}(x_j) = 0$;

(vi) $\mathrm{ad}(y_i)^{-\langle \alpha_j, \alpha_i \rangle + 1}(y_j) = 0$.

Serre's Theorem asserts that these relations suffice to completely determine L, i.e., L is isomorphic to the Lie algebra generated by elements $\{h_1, \dots, h_\ell, x_1, \dots, x_\ell, y_1, \dots, y_\ell\}$ subject to the above relations.

References

M. Auslander

[1] *On the Purity of the Branch Locus,* Amer. J. Math. 84 (1962), 116–125.

M. F. Atiyah and I. G. MacDonald

[1] *Introduction to Commutative Algebra,* Addison-Wesley, Reading, Mass., 1969.

C. T. Benson and L. C. Grove

[1] *Finite Reflection Groups*, Graduate Texts in Mathematics no. 99, Springer-Verlag, 1983.

D. J. Benson

[1] *Polynomial Invariants of Finite Groups*, LMS Lecture Note Series 190, Cambridge University Press, 1993.

A. Borel and J. de Siebenthal

[1] *Les sous-groupes fermés de rang maximum des groupes de Lie clos,* Comment. Math. Helv. 23 (1949), 200–221.

R. Bott

[1] *An Application of the Morse Theory to the Topology of Lie Groups*, Bull. Soc. Math. France 84 (1956), 251–282.

N. Bourbaki

[1] *Éléments de mathématique: Groupes et algèbres de Lie. Chapitres 4, 5 et 6,* Masson, 1981.

R. W. Carter

[1] *Simple Groups of Lie Type*, John Wiley and Sons, London, 1972.
[2] *Conjugacy Classes in the Weyl Groups*, Compositio Math. 25 (1972), 1–59.
[3] *Finite Groups of Lie Type*, John Wiley and Sons, New York, 1985.

C. Chevalley

[1] *Invariants of Finite Groups Generated by Reflections*, Amer. J. Math. 77 (1955), 778–782.

A. Clark and J. Ewing

[1] *The Realization of Polynomial Algebras as Cohomology Rings*, Pacific J. Math. 50 (1974), 425–434.

A. M. Cohen

[1] *Finite Complex Reflection Groups*, Ann. Sci. École Norm. Sup. 9 (1976), no. 3, 379–436.
[2] *Erratum "Finite Complex Reflection Groups"*, Ann. Sci. École Norm. Sup. 11 (1978), no. 4, 613.
[3] *Finite Quaternionic Reflection Groups*, J. Algebra 64 (1980), no. 2, 293–324.
[4] *Presentations for Certain Finite Quaternionic Reflection Groups*, Advances in finite geometries and designs (Chelwood Gate, 1990), 69–79, Oxford University Press, New York, 1991.
[5] *Recent Results on Coxeter Groups*, Polytopes: abstract, convex and computational (Scarborough, ON, 1993), 1–19, NATO Adv. Sci. Inst. Ser. C, Kluwer Acad. Publ., Dordrecht, 1994.

H. S. M. Coxeter

[1] *Discrete Groups Generated by Reflections*, Annals of Math. 35 (1934), 588–621.
[2] *The Product of the Generators of a Finite Group Generated by Reflections*, Duke Math. J. 18 (1951), 765–782.
[3] *Groups Generated by Unitary Reflections of Period Two*, Canad. J. Math. 9 (1957), 243–272.
[4] *Finite Groups Generated by Unitary Reflections*, Abh. Math. Sem. Univ. Hamburg 31 (1967), 125–135.

C. Curtis and I. Reiner

[1] *Representation Theory of Finite Groups and Associative Algebras*, John Wiley and Sons, London, 1962.

M. Demazure

[1] *Invariants symétriques entiers des groupes de Weyl et torsion*, Invent. Math. 21 (1973), 287–301.

V. V. Deodhar

[1] *On the Root System of a Coxeter Group*, Comm. Algebra 10 (1982), 611–630.

L. E. Dickson

[1] *A Fundamental System of Invariants of the General Modular Linear Group with a Solution of the Form Problem*, Trans. Amer. Math. Soc. 12 (1911), 274–286.

A. Dress

[1] *On Finite Groups Generated by Pseudoreflections*, J. Algebra 11 (1969), 1–5.

L. Flatto

[1] *Basic Sets of Invariants for Finite Reflection Groups*, Bull. Amer. Math. Soc. 74 (1968), 730–734.
[2] *Invariants of Finite Reflection Groups*, Enseign. Math. (2) 24 (1978), nos. 3–4, 237–292.

R. Hartshorne

[1] *Algebraic Geometry*, Graduate Texts in Mathematics no. 52, Springer-Verlag, 1977.

H. Hiller

[1] *Schubert Calculus of a Coxeter Group*, Enseign. Math. (2) 27 (1981), 57–84.
[2] *Geometry of Coxeter Groups*, Research Notes in Mathematics 54 (1982), Pitman.
[3] *Coinvariant Theory of a Coxeter Group*, The Geometric Vein, Springer-Verlag, 1981, 555–559.

M. Hochster and J. A. Eagon

[1] *Cohen-Macaulay Rings, Invariant Theory, and the Generic Perfection of Determinantal Loci*, Amer. J. Math. 93 (1971), 1020–1058.

K. Hoffman and R. Kunze

[1] *Linear algebra*, second edition, Prentice-Hall, 1971.

R. B. Howlett

[1] *Normalizers of Parabolic Subgroups of Reflection Groups*, J. London Math. Soc. (2) 21 (1980), 62–80.

J. E. Humphreys

[1] *Introduction to Lie algebras and Representation Theory*, Graduate Texts in Mathematics no. 9, Springer-Verlag, 1972.
[2] *Reflection Groups and Coxeter groups,* Cambridge Studies in Advanced Mathematics vol. 29, Cambridge University Press, 1990.

N. Iwahori and H. Matsumoto,

[1] *On Some Bruhat Decompositions and the Structure of the Hecke Ring of p-adic Chevalley Groups,* Inst. Hautes Études Sci. Publ. Math. no. 25 (1965), 5–48.

V. G. Kac

[1] *Torsion in Cohomology of Compact Lie Groups and Chow Rings of Reductive Algebraic Groups,* Invent. Math. 80 (1985), 69–79.

V. G. Kac and D. H. Peterson

[1] *Infinite Flag Varieties and Conjugacy Theorems,* Proc. Nat. Acad. Sci. U.S.A. 80 (1983), no. 6 i, 1778–1782.
[2] *Defining Relations of Certain Infinite-Dimensional Groups,* The mathematical heritage of Élie Cartan (Lyon, 1984). Astérisque 1985, Numéro Hors Série, 165–208.
[3] *Generalized Invariants of Groups Generated by Reflections,* Geometry Today (Rome, 1984), 231–249, Progr. Math. 60, Birkhäuser, 1985.
[4] *Constructing Groups Associated to Infinite-Dimensional Lie Algebras. Infinite-Dimensional Groups with Applications,* (Berkeley, Calif., 1984), 167–216, Math. Sci. Res. Inst. Publ. 4, Springer-Verlag, 1985.

K. Kendig

[1] *Elementary Algebraic Geometry,* Graduate Texts in Mathematics no. 44, Springer-Verlag, 1977.

B. Kostant

[1] *The Principal Three-Dimensional Subgroup and the Betti Numbers of a Complex Simple Lie Group,* Amer. J. Math. 81 (1959), 973–1032.

T. Y. Lam

[1] *A First Course in Noncommutative Rings*, Springer-Verlag, 1991.

S. Lang

[1] *Algebra,* second edition, Addison-Wesley Publishing Co., 1984.

G. Lusztig

[1] *A Class of Irreducible Representations of a Weyl Group,* Nederl. Akad. Wetensch. Indag. Math. 41 (1979), no. 3, 323–335.

[2] *A Class of Irreducible Representations of a Weyl Group. II,* Nederl. Akad. Wetensch. Indag. Math. 44 (1982), no. 2, 219–226.

I. G. MacDonald

[1] *On the Degrees of the Irreducible Representations of Symmetric Groups,* Bull. London Math. Soc. 3 (1971), 189–192.

[2] *Some Irreducible Representations of Weyl Groups*, Bull. London Math. Soc. 4 (1972), 148–150.

[3] *The Poincaré Series of a Coxeter Group*, Math. Ann. 199 (1972), 161–174.

[4] *On the Degrees of the Irreducible Representations of Finite Coxeter Groups*, J. London Math. Soc. 6 (1973), 298–300.

J. Milnor and J. C. Moore

[1] *On the Structure of Hopf Algebras*, Annals of Math 81 (1965), 211–264.

M. Nagata

[1] *Local Rings*, Interscience Tracts in Pure and Applied Mathematics no. 13, John Wiley and Sons, 1962.

F. Neumann, M. D. Neusel, and L. Smith

[1] *Rings of Generalized and Stable Invariants of Pseudoreflections and Pseudoreflection Groups*, J. Algebra 182 (1996), no. 1, 85–122.

M. D. Neusel and L. Smith

[1] *Polynomial Invariants of Groups Associated to Configurations of Hyperplanes over Finite Fields,* J. Pure Appl. Algebra 122 (1997), nos. 1–2, 87–105.

P. Orlik and L. Solomon

[1] *Unitary Reflection Groups and Cohomology,* Invent. Math. 59 (1980), no. 1, 77–94.
[2] *Discriminants in the Invariant Theory of Reflection Groups,* Nagoya Math. J. 109 (1988), 23–45.
[3] *The Hessian map in the Invariant Theory of Reflection Groups,* Nagoya Math. J. 109 (1988), 1–21.

A. Pianzola and A. Weiss

[1] *Monstrous E_{10}'s and a Generalization of a Theorem of L. Solomon*, C. R. Math. Rep. Acad. Sci. Canada 11 (1989), no. 5, 189–194.

M. Reid

[1] *Undergraduate Algebraic Geometry*, LMS Student Texts vol. 12, Cambridge University Press, 1988.

R. W. Richardson

[1] *Conjugacy Classes of Involutions in Coxeter Groups*, Bull. Austral. Math. Soc. 26 (1982), 1–15.

C. Schoeller

[1] *Groupes affines, commutatifs, unipotents sur un corps non parfait*, Bull. Soc. Math. France 100 (1972), 241–300.

J. P. Serre

[1] *Groupes finis d'automorphisms d'anneaux locaux réguliers*, Colloq. d'Alg. École Norm. de Jeunes Filles, Paris (1967), 1–11.
[2] *Linear Representations of Finite Groups*, Graduate Texts in Mathematics no. 42, Springer-Verlag, 1977.

G. C. Shephard and J. A. Todd

[1] *Finite Unitary Reflection Groups*, Canad. J. Math. 6 (1954), 274–304.

G. C. Shephard

[1] *Unitary Groups Generated by Reflections,* Canad. J. Math. 5 (1953), 364–383.
[2] *Some Problems on Finite Reflection Groups,* Enseign. Math. (2) 2 (1956), 42–48.
[3] *Abstract Definitions for Reflection Groups,* Canad. J. Math. 9 (1957), 273–276.

L. Smith

[1] *On the Invariant Theory of Finite Pseudoreflection Groups,* Arch. Math. (Basel) 44 (1985), 225–228.
[2] *On the Invariant Theory of Finite Groups: Orbit Polynomials and Splitting Principles,* J. Algebra 110 (1987), no. 1, 134–157.
[3] *Polynomial Invariants of Finite Groups,* Research Notes in Mathematics no. 6, A. K. Peters, 1995.
[4] *Some Rings of Invariants that are Cohen-Macaulay,* Canad. Math. Bull. 39 (1996), 238–240.
[5] *Polynomial Invariants of Finite Groups. A Survey of Recent Developments,* Bull. Amer. Math. Soc. 34 (1997), no. 3, 211–250.

L. Solomon

[1] *Invariants of Finite Reflection Groups,* Nagoya J. Math. 22 (1963), 57–64.
[2] *Invariants of Euclidean Reflection Groups,* Trans. Amer. Math. Soc. 113 (1964), 274–286.
[3] *The Orders of the Finite Chevalley Groups,* J. Algebra 3 (1966), 376–393.
[4] *A Decomposition of the Group Algebra of a Finite Coxeter Group,* J. Algebra 9 (1968), 220–239.

T. A. Springer

[1] *Some Arithmetical Results on Semi-Simple Lie Algebras,* Inst. Hautes Études Sci. Publ. Math. no. 30 (1966), 115–141.
[2] *Regular Elements of Finite Reflection Groups,* Invent. Math. 25 (1974), 159–198.
[3] *Invariant Theory,* Lecture Notes in Mathematics vol. 585, Springer-Verlag, 1977.
[4] *Some Remarks on Involutions in Coxeter Groups,* Comm. Algebra 10 (1982), 631–636.
[5] *On Representations of Weyl Groups,* Proceedings of the Hyderabad Conference on Algebraic Groups (Hyderabad, 1989), 517–536, Manoj Prakashan, Madras, 1991.

R. P. Stanley

[1] *Relative Invariants of Finite Groups Generated by Pseudo Reflections*, J. Algebra 49 (1977), 134–148.
[2] *Invariants of Finite Groups and their Applications to Combinatorics*, Bull. Amer. Math. Soc. 1 (1979), 475–511.

R. Steinberg

[1] *Invariants of Finite Reflection Groups*, Canad. J. Math. 12 (1960), 616–618.
[2] *Differential Equations Invariant under Finite Reflection Groups*, Trans. Amer. Math. Soc. 112 (1964), 392–400.
[3] *Endomorphisms of Linear Algebraic Groups*, Memoirs Amer. Math. Soc. 80 (1968), 1–108.
[4] *Torsion in Reductive Groups*, Advances in Math. 15 (1975), 63–92.
[5] *On Dickson's Theorem on Invariants*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 34 (1987), 699–707.

H. Toda

[1] *Cohomology mod 3 of the Classifying Space BF_4 of the Exceptional Group F_4*, J. Math. Kyoto Univ. 13 (1973), 97–115.

W. V. Vasconcelos

[1] *Ideals Generated by R-Sequences*, J. Algebra 6 (1967), 309–316.

C. A. Weibel

[1] *An Introduction to Homological Algebra*, Cambridge Studies in Advanced Mathematics vol. 38, Cambridge University Press, 1994.

C. W. Wilkerson

[1] *A Primer on the Dickson Invariants*, Proceedings of the Northwestern Homotopy Theory Conference (Evanston, Ill., 1982), 421–434, Contemp. Math. vol. 19, Amer. Math. Soc., 1983.

Index